МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА СИСТЕМ ІНФОРМАЦІЙНОГО ТА КІБЕРНЕТИЧНОГО ЗАХИСТУ

«На правах рукопису»
УДК 681.3.06

«До захисту допущено»
Завідуючий кафедрою СІКЗ
_____к.т.н. Г.В. Шуклін
«____» _____2023 р.

БАКАЛАВРСЬКА АТЕСТАЦІЙНА РОБОТА

зі спеціальності 125 “Кібербезпека”

на тему: **РОЗРОБКА СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ У РЕАЛЬНОМУ МАСШТАБІ ЧАСУ**

Студент групи СЗД-4 Сиротинський Володимир Юрійович

_____
(підпис)

Науковий керівник: к.т.н., доц Пепа Юрій Володимирович _____
(підпис)

Нормоконтроль ст. викл. Зозуля Сергій Анатолійович _____
(підпис)

КИЇВ – 2023

«ЗАТВЕРДЖУЮ»
Завідувач кафедри СІКЗ
_____ к.т.н. Г.В. Шуклін
(підпис)
«_____»_____ 2023р.

ЗАВДАННЯ

на атестаційну роботу бакалавра

студенту: Сиротинському Володимиру Юрійовичу

1.Тема роботи: Розробка системи виявлення вторгнень у реальному масштабі часу, затверджено наказом від «24 » лютого 2023р. № 26

2.Термін здачі студентом оформленої роботи «____» _____ 2023р.

3. Об'єкт дослідження: процеси забезпечення захисту інформації від кібератак на об`єтах критичної інформаційної інфраструктури.

4. Предметом дослідження: технології захисту, які забезпечують інформаційну безпеку об`єктів критичної інфраструктури.

5. Мета роботи: аналіз моделей і методики, що використовуються для атрибуції порушників кібербезпеки в інтересах побудови перспективної системи атрибуції під час реалізації цільових атак на об'єкти критичної інформаційної інфраструктури.

6.Перелік питань, які мають бути розроблені:

Для досягнення вказаної мети виконуються такі основні задачі:

- аналіз існуючих вторгнень на об`єкти критичної інфраструктури;
- аналіз та дослідження існуючих методів захисту від вторгнень на критичні інформаційні об`єкти критичної інфраструктури;
- створення рекомендацій щодо забезпечення інформаційної безпеки від кібератак на критичних об`єктах інформаційної інфраструктури.

7. Дата видачі завдання «____» _____20____р.

Науковий керівник _____ Шуклін Г.В.
(підпис)

Завдання прийняла до виконання _____Сиротинський В.Ю.

(підпис)

КАЛЕНДАРНИЙ ПЛАН

Дата видачі завдання «24» лютого 2023р.

№ з/п	Назва етапів дипломної роботи	Строк виконання етапів роботи	Примітка
1	Підбір науково-технічної літератури	до 26.02.23р.	
2	Обґрунтування актуальності теми роботи	до 27.02.23р.	
3	Написання першого розділу роботи	до 16.03.23р.	
4	Написання другого розділу роботи	до 12.04.23р.	
5	Написання третього розділу роботи	до 08.05.23р.	
6	Написання висновків по роботі	до 11.05.23р.	
8	Підготовка демонстраційних матеріалів	до 18.05.23р.	
9	Підготовка доповіді	до 24.05.23р.	
10	Захист в ДЕК		

Студентка: СЗД -41 Сиротинський В.Ю. _____
(підпис)

Науковий керівник: к.т.н., доц. Шуклін Г.В. _____
(підпис)

Нормоконтроль: ст. викл. Зозуля С.А. _____
(підпис)

ЗМІСТ

РЕФЕРАТ

Дипломна робота містить 48 сторінок, 15 рисунки, 1 таблиця.

На основі розгляду відкритих джерел у роботі представлено аналіз моделей і методики, які використовуються для атрибуції кіберзлочинців під час реалізації цільових атак, і які застосовуються як у наукових, так і в практичних проектах. У роботі проведено аналіз нових моделей, що використовуються для атрибуції, які дають змогу здійснювати збір даних на тактико-технічному рівні. Виокремлено основні показники кібератак і порушників, що проводяться, суттєві для реалізації процесів атрибуції. Розглянуто порядок формування даних для профілювання кіберзлочинних угрупувань, а також можливості застосування розглянутих моделей і методики в інтересах побудови перспективної системи атрибуції кіберзловмисника під час реалізації цільових атак на об'єкти критичної інформаційної інфраструктури. Аналіз виконано за джерелами за двадцятирічний період, тим часом основні роботи, що розглядаються, були опубліковані за останні п'ять років. Аналіз не претендує на повноту, але робиться спроба охопити найбільш значущі дослідження.

Об’єктом дослідження: процеси забезпечення захисту інформації від кібератак на об`єтах критичної інформаційної інфраструктури.

Предметом дослідження є технології захисту, які забезпечують інформаційну безпеку об`єктів критичної інфраструктури.

Мета роботи аналіз моделей і методики, що використовуються для атрибуції порушників кібербезпеки в інтересах побудови перспективної системи атрибуції під час реалізації цільових атак на об'єкти критичної інформаційної інфраструктури.

Для досягнення вказаної мети виконуються такі основні задачі:

- аналіз існуючих вторгнень на об`єкти критичної інфраструктури;
- аналіз та дослідження існуючих методів захисту від вторгнень на критичні інформаційні об`єкти критичної інфраструктури;

- створення рекомендацій щодо забезпечення інформаційної безпеки від кібератак на критичних об`єктах інформаційної інфраструктури.

ABSTRACT

Thesis contains 48 pages, 15 figures, 1 tables

Based on the review of open sources, the paper presents an analysis of models and methodologies used to attribute cybercriminals during targeted attacks, which are used in both scientific and practical projects. The paper analyzes the new models used for attribution, which allow collecting data at the tactical and technical level. The main indicators of cyberattacks and perpetrators that are essential for the implementation of attribution processes are highlighted. The procedure for generating data for profiling cybercriminal groups, as well as the possibility of applying the considered models and methods in the interests of building a promising system of cyberattacker attribution in the course of targeted attacks on critical information infrastructure facilities are considered. The analysis is based on sources for a twenty-year period, while the main works under consideration were published in the last five years. The analysis does not claim to be complete, but an attempt is made to cover the most significant studies.

Object of research: processes for ensuring the protection of information from cyberattacks at critical information infrastructure facilities.

The subject security technologies that ensure information security of critical infrastructure facilities.

The purpose analysis of models and methodologies used for attribution of cybersecurity offenders in the interests of building a promising attribution system for targeted attacks on critical information infrastructure.

To achieve this goal, the following main tasks are performed:

- analysis of existing intrusions into critical infrastructure facilities;

- analysis and research of existing methods of protection against intrusions on critical information objects of critical infrastructure;

- development of recommendations for ensuring information security against cyberattacks on critical information infrastructure facilities.

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

БЛОС	Бездротові локальні обчислювальні системи	Wireless local cleaning systems
ОІД	Об`єкт інформаційної діяльності	Object of information activity
СІЗ	Системи інформаційного захисту	Information protection systems
EEPROM	Постійний запам’ятовувач що програмується та очищується за допомогою електрики	Electrically Erasable Programmable Read-Only Memory
NIST	Національний інститут стандартизації та технологій	The National Institute of Standards and Technology
PKI	Інфраструктура публічних ключів	Public key infrastructure
RAM	Пам’ять з довільним доступом	Random Access Memory
RFID	Радіочастотна ідентифікація	Radio frequency identification
ROM	Пам’ять лише для читання	Read Only Memory
SRAM	Статична оперативна пам’ять з довільним доступом	Static random access memory
TDMA	Метод часового поділу	Time division multiple access
WLAN	Метод часового поділу	Wireless Local Area Network
ВЧ	Високі частоти	
ЗЗІ	Засоби захисту інформації	
ІС	Інформаційна система	

ІТС	Інформаційно-телекомунікаційна система
ОЗП	Оперативний запам’ятовувальний пристрій
УВЧ	Ультра високі частоти

ВСТУП

Країни НАТО на саміті 2022 року у Парижі визнали, що кібератака може завдати шкоди, яку можна порівняти зі шкодою від збройного нападу, а кіберпростір оголосили галуззю, що дорівнює іншим звичайним військовим галузям - суходолу, морю і повітрю. Приводом послужили кібератаки, що вплинули на цілісність суверенітету низки держав. У міру того, як технології стають дедалі продвинутими і складнішими, змінюються і методики, які використовують у сучасних кібератаках. Засоби захисту інформації, що застосовуються проти традиційних загроз безпеки, часто є неефективними проти сучасних цільових кібератак. Це пов'язано з тим, що кіберпорушники, які стоять за вторгненням, зосереджені на конкретній меті та мають змогу адаптуватися до прийнятих захисних методів і засобів реагування на інциденти. Метою порушників найчастіше стають критична інформаційна інфраструктура (КІІ) або об'єкти КІІ. Одним із найважливіших інструментів стримування державних агресій і проведення цілеспрямованих кібероперацій є здатність здійснювати ефективну атрибуцію порушника, під якою розуміють процес ідентифікації порушника, який реалізовував кібератаку, його цілей, мотивів, виконуваних дій і засобів реалізації атаки, що використовуються.

Здебільшого атрибуція порушників здійснюється після здійснення кібератаки і переважно ручним методом. Основу традиційної атрибуції становить аналіз методів і засобів, що застосовуються порушниками. Можливість ефективної автоматизованої та інтелектуальної атрибуції в реальному часі робить наукове завдання дослідження та побудови ефективних систем атрибуції порушників перспективним для досліджень. Для цього необхідний розгорнутий аналіз сучасних моделей, що використовуються для атрибуції, в інтересах побудови перспективної системи атрибуції порушника під час цільових атак на КІІ.

Актуальність теми Нині збільшується кількість цільових кібератак на КІІ. Однак чіткого визначення та єдиних критеріїв, що дозволяють відносити різні типи кібератак до цільових, серед експертів досі не визначено. Цільові

кібератаки необхідно відрізняти від інших традиційних кібератак, до яких відносяться атаки випадкового характеру і широкого фокусу, спрямовані на компрометацію великої кількості користувачів і систем. Кіберпорушники, які здійснюють цільові кібератаки, чітко розділяють цілі в очікуванні необхідного моменту для організації запланованого сценарію атаки. У них є певні наміри. У більшості випадків - це фінансова вигода, порушення технологічних процесів, промислове шпигунство, крадіжка інтелектуальної власності, саботаж КІІ. Цільові кібератаки структуровані й технологічно просунуті. Атакуюча сторона високо мотивована і володіє необхідними професійними навичками. У сукупності ці фактори утворюють необхідний базис для цільових кібератак.

Об’єктом дослідження: процеси забезпечення захисту інформації від кібератак на об`єтах критичної інформаційної інфраструктури.

Предметом дослідження є технології захисту, які забезпечують інформаційну безпеку об`єктів критичної інфраструктури.

Мета роботи аналіз моделей і методики, що використовуються для атрибуції порушників кібербезпеки в інтересах побудови перспективної системи атрибуції під час реалізації цільових атак на об'єкти критичної інформаційної інфраструктури.

Для досягнення вказаної мети виконуються такі основні задачі:

- аналіз існуючих вторгнень на об`єкти критичної інфраструктури;
- аналіз та дослідження існуючих методів захисту від вторгнень на критичні інформаційні об`єкти критичної інфраструктури;
- створення рекомендацій щодо забезпечення інформаційної безпеки від кібератак на критичних об`єктах інформаційної інфраструктури.

РОЗДІЛ 1 АНАЛІЗ МОДЕЛЕЙ І МЕТОДИК, ЯКІ ВИКОРИСТОВУЮТЬСЯ ДЛЯ АТРІБУЦІЇ ПОРУШНИКІВ КІБЕРБЕЗПЕКИ ПРИ РЕАЛІЗАЦІЇ ЦІЛЬОВИХ АТАК

1.1. Цільові атаки та атрибуції

В багатьох випадках цільові кібератаки позначають як *APT* (*Advansed Persistent Threats*) - просунуті постійні загрози. Експерти стверджують, що цільові кібератаки не завжди мають характер просунутих постійних загроз. Відмітна характеристика *APT* - адаптація до захисних заходів і пошук нових слабких місць у системі безпеки об'єкта атаки. Як правило, порушник володіє значними ресурсами, які дозволяють йому створювати можливості для досягнення цілей за допомогою різних векторів вторгнення і залишатися непоміченим у скомпрометованій системі тривалий час. Такі кібератаки, здебільшого, є санкціонованими урядом спеціалізованими компаніями, що виконуються переважно на інформаційно-телекомунікаційну інфраструктуру військових і державних об'єктів. Найчастіше в проведенні цільових шкідливих компаній підозрюють спецслужби інших країн і загони "урядових хакерів" . Саме такі атаки, які реалізує противник із високим рівнем знань і вмінь, що володіє значними ресурсами для використання безлічі різних векторів атак, що діє для досягнення деякої кінцевої мети, необхідно класифікувати як *APT* . Узагальнюючи все сказане вище, цільові кібератаки - це клас спеціалізованих, багаторівневих атак, спрямованих на обмежений і заздалегідь обраний набір цінних активів або фізичних систем з явною метою крадіжки, компрометації конфіденційних даних або саботажу систем. Цей тип кібератак містить у собі структурований комплекс заходів, формуючи життєвий цикл цільової атаки.

Атрибуція кібератаки - це процес ідентифікації походження і джерела кібератаки з метою встановлення зловмисника або групи зловмисників, які ініціювали атаку. Інакше кажучи, під атрибуцією кібератаки розуміють процес встановлення злочинця, який реалізує кібератаки щодо об'єкта деструктивного впливу.

Ландшафт кіберзагроз, що постійно змінюється, і стрімке зростання екосистеми ринків *даркнету* дали змогу застосовувати на практиці схожий інструментарій, ускладнюючи ідентифікацію конкретного кібероугруповання. Методи заплутування аналітиків і аналітичних систем під час розслідування інциденту також ускладнюють атрибуцію. *APT* намагаються підробляти час компіляції, працюють у неробочий час, впроваджують різні мови або унікальні культурні свідоцтва в рядки коду, повторно реєструють командно-керувальні домени, які використовували раніше, інших зловмисників тощо. Застосовується універсальне програмне забезпечення (ПЗ), яке ефективне під час досягнення короткострокової мети або виконання вузько спрямованого завдання. Таке ж ПЗ використовують як кіберугруповання, так і окремі порушники. Оскільки в більшості випадків застосовується одне й те саме ПЗ, з'ясувати, чи стоїть за цільовою кібератакою *APT*, чи звичайний зловмисник дуже проблематично. Відповідно, свідчення і докази, що застосовуються для атрибуції атак, можна підробити і замаскувати, тим самим ускладнивши атрибуцію. Виділимо основні проблеми атрибуції:

- постійне прогресування *APT*;

- визначення джерел, тобто місць запуску та ініціалізації кібератаки;
- визначення відповідального за кібератаку основного актора);
- обробка великої кількості несортованих, тобто початкових даних;
- децентралізація і заплутаність наявних систем публічно-приватної атрибуції;
- використання методів імітації кібератак з метою формування неправдивих звинувачень конкретного порушника, кіберугруповання та держави;
- *APT* в багатьох випадках застосовують певні методи і сценарії реалізації атаки, вибудовуючи необхідне середовище для досягнення поставлених цілей, виконують розподілену узгоджену послідовність складно етапів, які пройшли обстеження, можливо кілька залежних або незалежних ланцюжків дій.

1.2. Моделі, які використовуються для атрибуції

Модель Cyber Kill Chain

Щоб краще розуміти й аналізувати *APT*, було розроблено описову модель *Cyber Kill Chain* (*СКС*, "*ланцюжок кібервторгнень*") та її розширену версію. Основою для моделі послугувала концепція *Kill Chain* (*Ланцюжок вбивств*), яку вперше прийняли військові для опису дій, що використовуються противником для атаки і знищення цілі.

Розпізнавання етапів *СКС* дає можливість ідентифікувати зловмисників і вжити заходів у відповідь. Використовуючи цю модель, компанія *Lockheed Martin* розробила власну модель *СКС*.

СКС - це схематичний опис послідовних кроків порушника у вигляді взаємопов'язаних ланок ланцюга. Модель спрямована на вивчення поведінки порушника.

Базова версія моделі *СКС* передбачає сім кроків, необхідних для реалізації успішної кібератаки, як це представлено на рисунку 1.1.:

1) розвідка;

2) озброєння;

3) доставка;

4) експлуатація;

5) установка;

6) командування і контроль;

7) виконання дій.

Модель *СКС* описує атаку зовнішнього зловмисника, який намагається отримати доступ до даних або активів усередині периметра цільового об'єкта. Зловмисник виконує розвідку, вторгнення, використання вразливостей. Далі йде отримання і підвищення привілеїв, переміщення для доступу до цінніших активів. На фінальній стадії робиться спроба приховування своєї активності, і

проводиться ексфільтрація (потайне вивантаження) необхідних даних за межі цільового середовища.

Пропонований підхід дає змогу експертам ідентифікувати методи та засоби, що застосовуються зловмисниками на кожному етапі кібератаки.

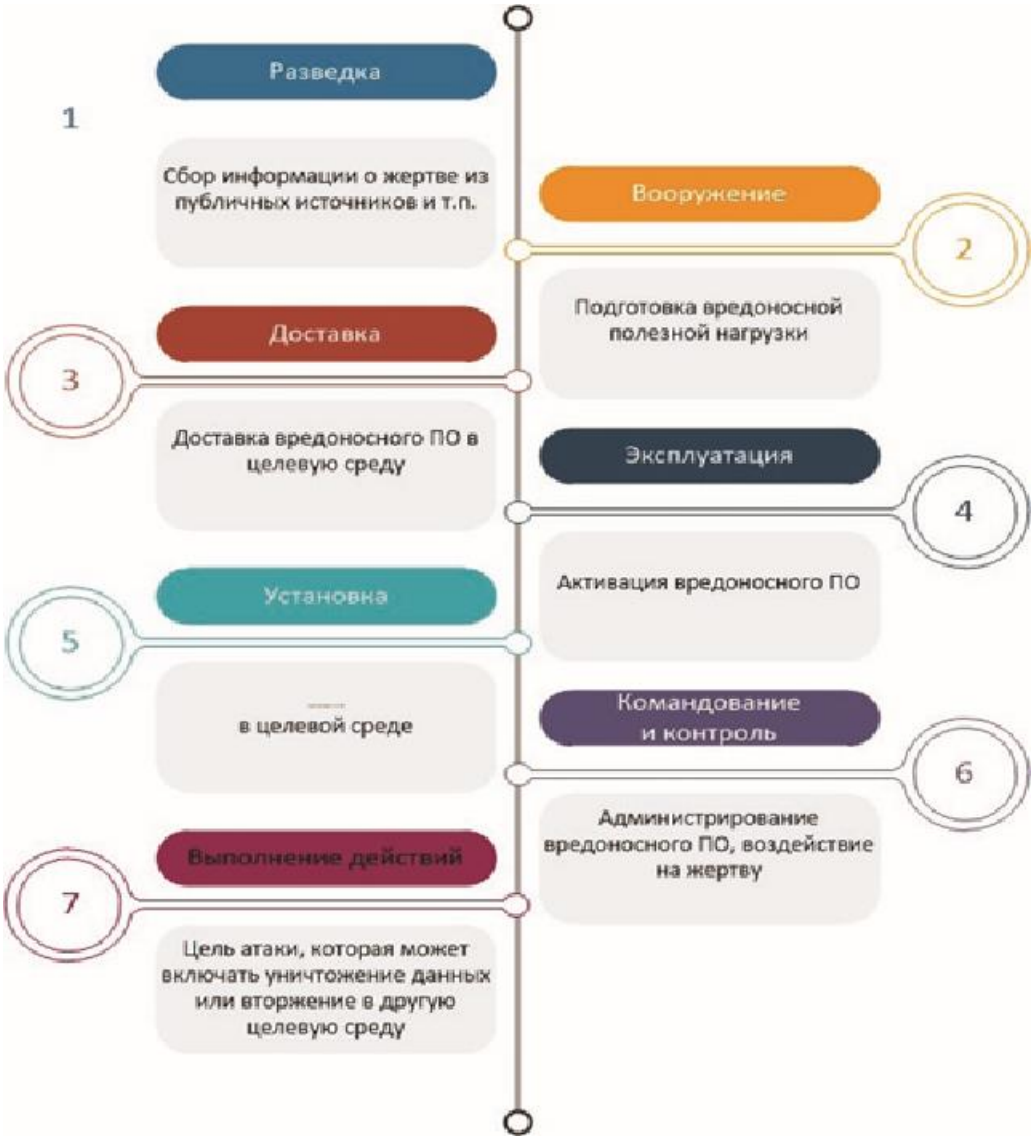

Рисунок 1.1. Етапи базової моделі *СКС*.

Базова модель неодноразово піддавалася дослідниками модернізації для застосування в різних галузях, зокрема й для кіберфізичних систем. Традиційна модель *СКС* орієнтована на облік периметра цільового об'єкта і використання шкідливого програмного забезпечення (ПЗ). Таким чином, ця модель не охоплює інші вектори атак, що відбуваються за периметром цільового об'єкта.

Модель Unifid Kill Chain

З урахуванням векторів атак та інструментарію порушника, що постійно нарощуються, кількість етапів було збільшено до вісімнадцяти, і така модель отримала назву *Unifid Kill Chain* (*U K C*, "*уніфікований ланцюжок кібервторгнень*").

У розширеній версії моделі ланцюжок етапів представлено на рисунку 1.2.

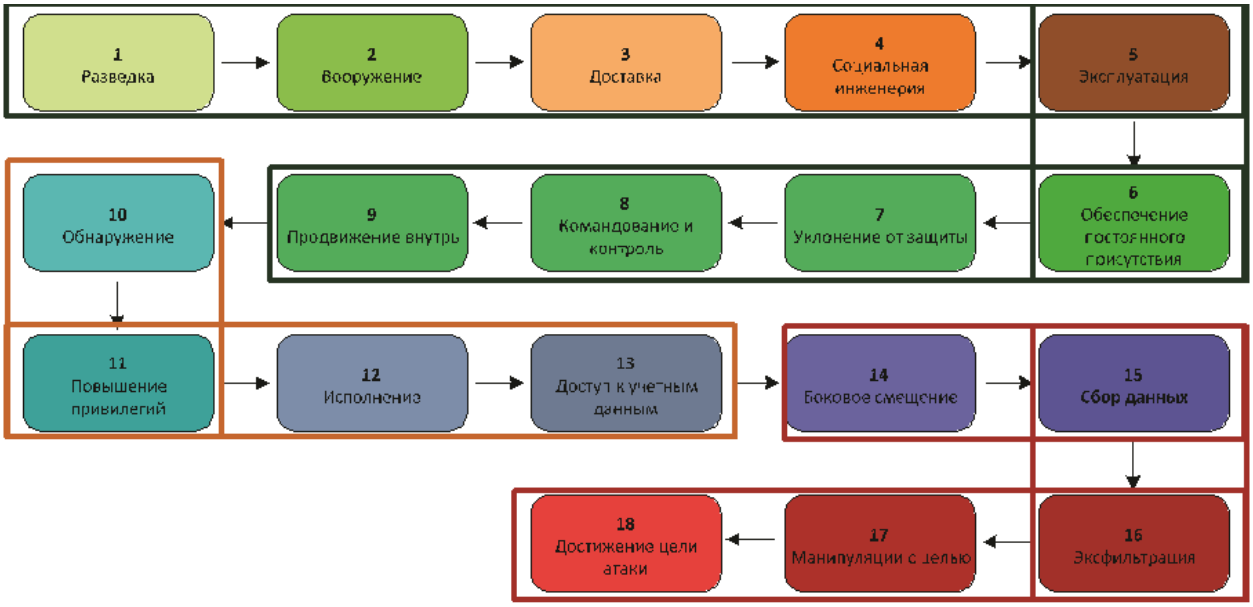

Рисунок 1.2. Кроки розширеної моделі *U K C*

Розглянемо ці кроки.

Крок 1. **Розвідка.** На цьому кроці здійснюється збір інформації про атаковану ціль. Встановлюється організаційна структура, застосовані інформаційні технології, засоби захисту від того, що зловмисники намагатимуться ідентифікувати та дослідити наявні між мережеві екрани, системи запобігання вторгненням, механізми автентифікації тощо. Для виявлення "вузьких" місць і визначення найменш захищених елементів служб та сервісів в інформаційно-комунікаційній інфраструктурі потенційної жертви аналізуються технологічні процеси. У випадку з об'єктами КІІ, проводиться можлива оцінка шкоди національним і стратегічним інтересам держави. Отримана інформація виступає в ролі бази даних і знань під час виконання наступного кроку.

Етап 2. **Озброєння**. Виконуються підготовчі заходи, спрямовані на створення інфраструктури, необхідної для атаки. Використовується наявне або

розробляється власне унікальне шкідливе ПЗ, зокрема експлойти, шифрувальники тощо.

Крок 3. **Доставка.** Активна фаза атаки, головне завдання якої впровадження і поширення застосовуваного шкідливого рішення в цільовому середовищі.

Крок 4. **Соціальна інженерія**. Застосовуються методи, спрямовані на маніпулювання персоналом (користувачами) з метою вчинення необхідних зловмиснику для здійснення небезпечних дій.

Крок 5. **Експлуатація**. Активація шкідливого рішення на скомпрометованому цільовому об'єкті. На етапі експлуатації зловмисники шукають додаткові вразливості або слабкі місця, які вони можуть використовувати в системах організації. Наприклад, ззовні зловмисник може не мати доступу до баз даних, але після вторгнення він може побачити, що база даних використовує стару версію ПЗ і схильна до добре відомої вразливості.

Крок 6. **Забезпечення постійної присутності**. Здійснюється будь-який доступ, дія або зміна в довіреному середовищі з метою забезпечення тривалої (постійної) присутності зловмисника в цільовій системі.

Крок 7. **Ухилення від захисту**. Застосовуються методи і засоби для обходу засобів захисту і приховування присутності в цільовій системі.

Крок 8. **Командування та контроль**. Здійснюється адміністрування шкідливого рішення, його оновлення, отримання нового функціоналу, реалізація повного спектра команд для досягнення поставлених цілей.

Крок 9. **Просування всередину**. Зловмисники встановлюють доступ через контрольовану систему в інші системи, до яких немає прямого доступу. ***Крок 10.*** **Виявлення**. Застосовуються методи і засоби, що дають змогу зловмиснику орієнтуватися в системі-жертві для подальших дій, отримувати інформацію про цільову систему, мережеве оточення і нові можливості. ***Крок 11.*** **Підвищення привілеїв**. Реалізуються методи і засоби, які дають змогу зловмиснику отримати ширші права в цільовій системі. Мета порушника - отримати привілеї для додаткових систем або облікових записів. Здійснюються

атаки методом грубої сили, пошук незахищених сховищ облікових даних, здійснюється стеження за незашифрованим мережевим трафіком тощо.
Крок 12. **Виконання**. Застосовуються методи і засоби, що дають змогу виконувати шкідливий код у локальній або віддаленій системі.
Крок 13. **Доступ до облікових даних**. Використовуються методи і засоби, що забезпечують доступ або контроль над обліковими даними системи, служби або домену.

Крок 14. **Бічне зміщення**. Використовується методика отримання порушниками доступу до інших віддалених систем, під'єднаних до скомпрометованого цільового середовища, для управління або деструктивного впливу, пошуку конфіденційної інформації або доступу до критично важливих активів. Під час бічного зміщення зловмисник часто використовує вразливості нульового дня або конфіденційні дані з віддалених систем без застосування спеціалізованого інструментарію.
Крок 15. **Збір даних**. Здійснюються ідентифікація та збір необхідних конфіденційних даних із цільової мережі.

Крок 16. **Ексфільтрація**. Використовуються методи і засоби прихованого вивантаження даних за межі цільового середовища. Вони сприяють крадіжці конфіденційних даних або видаленню даних із цільової мережі, тобто намагання замести сліди. Ексфільтрація може охоплювати такі методи, як обфускація (наприклад, за допомогою фальсифікації тимчасових міток, видалення або зміни журналів, маніпуляції в системі безпеки, щоб приховати попередні етапи в ланцюжку знищення і створити враження, що конфіденційних даних або систем не торкнулися тощо), відмова в обслуговуванні або шифрування.
Крок 17. **Маніпуляції з метою атаки**. Реалізуються методи і засоби маніпулювання, переривання або знищення цільової системи і (або) даних (атаки на доступність і цілісність) для досягнення кінцевої мети і (або) приховування слідів.
Етап 18. **Досягнення мети**. Виконання дій з реалізації кібератаки, спрямованих на досягнення мети реалізації кібератаки.

Модель *UKC* передбачає, що *APT* може не пройти всі можливі етапи, і деякі етапи можуть повторюватися. Наприклад, якщо на етапі ухилення від захисту порушника було виявлено, відбудеться коригування застосованих методів із метою проходження цього етапу доти, доки не буде досягнуто мети реалізації кібератаки. Повторюваний набір дій з досягнення мети може бути представлений у вигляді "*петлі*" , як це представлено на рисунку 1.3.

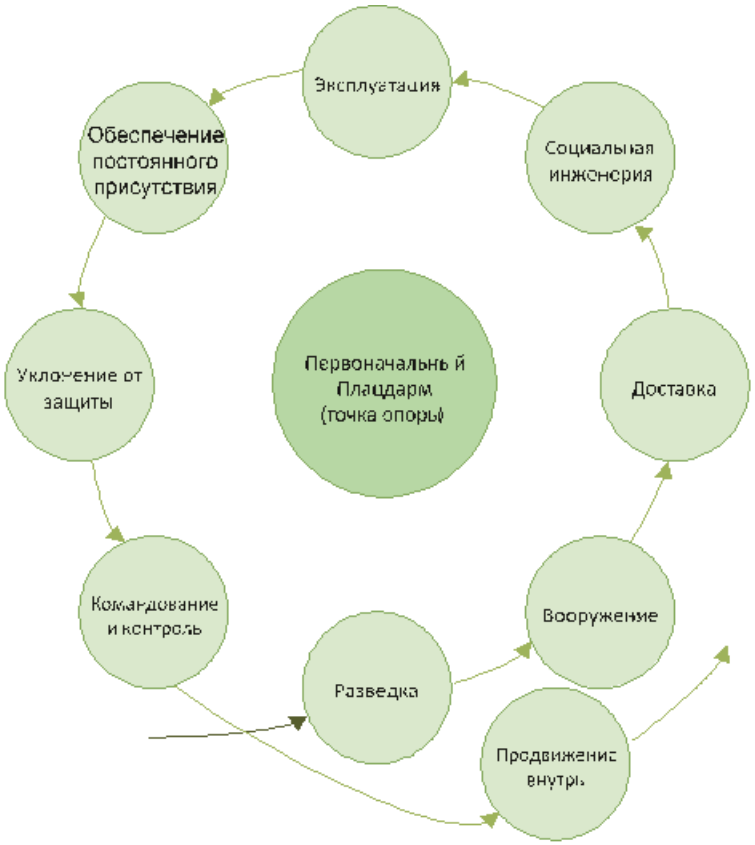

Рисунок 1.3. Представлення кроків реалізації кібератаки у вигляді *петлі* .

Модель *UKC* дає розуміння складних кібератак, що являють собою *APT* . Під час їх реконструкції кожен етап можна розбити на окремі блоки, характерні для конкретної *APT* . Блоки можуть характеризуватися індивідуальними атрибутами включаючи специфікацію поведінки, використовуваних методів та засобів.

За допомогою аналізу "*петлі*" на окремих фазах атаки в міру її реалізації можна визначити загальну кількість спроб досягнення мети реалізації

кібератаки. Ця інформація дасть змогу сформувати значення атрибутів "Наполегливість" або "Інтенсивність", що характеризують порушника (або *APT*). Також у поєднанні із застосовуваними методами і засобами можна означити атрибути "Майстерність" або "Технічний рівень". Загальну кількість підсумкового часу, необхідного на підготовку, можна враховувати для визначення значення атрибута "Час".

Модель Diamond

На рисунку 1.4. представлено модель аналізу вторгнень *Diamond* .

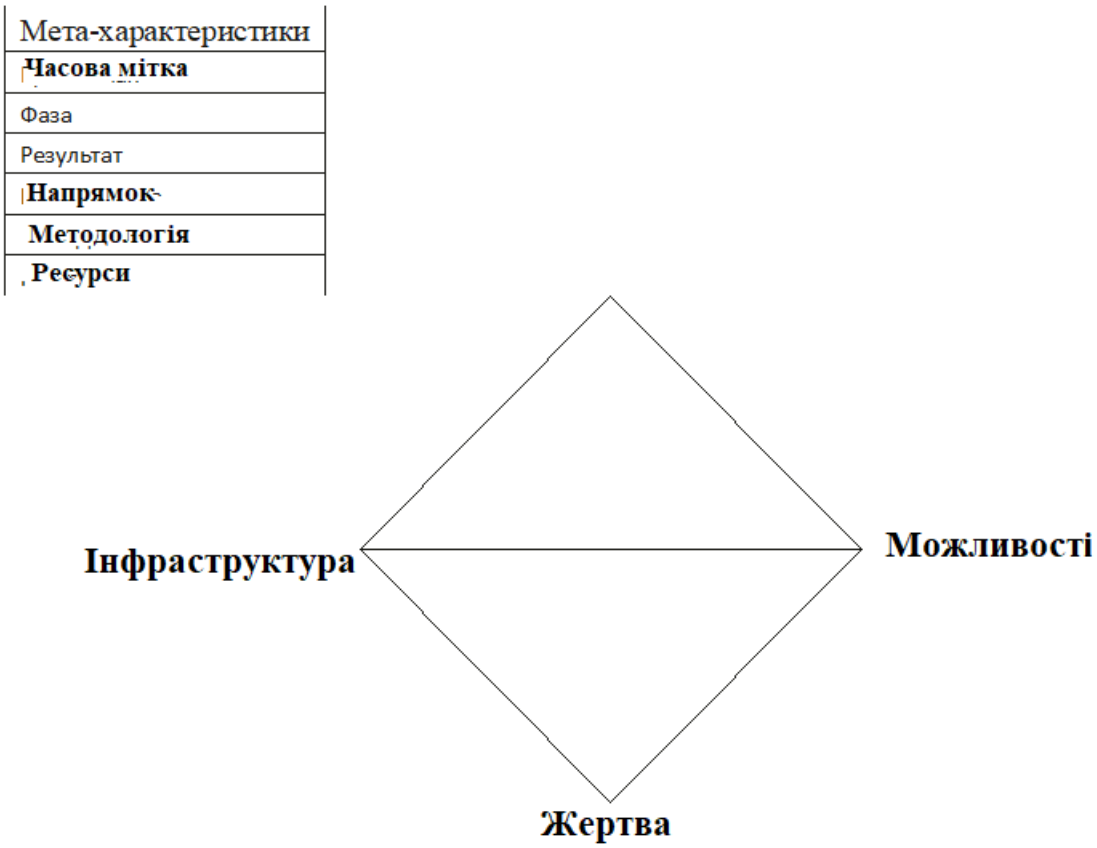

Рисунок 1.4. Модель аналізу вторгнень *Diamond*

Відповідно, враховуючи витрачений час, можна постаратися спрогнозувати деструктивний вплив і підсумкові наслідки. На основі даних, отриманих під час аналізу залишених слідів, артефактів, а також періоду до виявлення *APT* , також можна визначити атрибут "*Непомітність*". Інформація про атакований цільовий

об'єкт КІІ використовується для визначення атрибута "*Спеціалізація*". Залежно від приналежності до тієї чи іншої категорії КІІ, можна визначити атрибут, що характеризує вміння долати захисні заходи і проникати в цільову систему, наприклад "*Нестримність*". Підсумкові наслідки можуть відображати рівень агресії та інші атрибути результатів виконання *APT*. Порівняння різних ланцюжків реалізації кібератаки дає можливість виявити схожість або відмінність окремих ланцюжків. За підсумками аналізу формується профіль *APT*.

Варто зазначити, що проаналізовані моделі мають достатній набір характеристик, необхідних для досліджень цільових атак (*APT*). Вони дають змогу сформувати профіль порушника на абстрактному рівні. Досліджуючи ланцюжок етапів, експерти та аналітики можуть зрозуміти фази *APT*, джерела збору даних, вектори атаки, визначити застосовувані методики реалізації атаки і використовуваний інструментарій. Отримані відомості допоможуть сформувати профіль порушника, ідентифікувати метрики для своєчасного визначення етапів ланцюжка кібератак і виявити можливість реалізації атрибуції. Отримані під час аналізу кожного життєвого циклу періоду до виявлення *APT*, також можна визначити атрибут "*Непомітність*". Інформація про атакований цільовий об'єкт КІІ використовується для визначення атрибута "*Спеціалізація*". Залежно від приналежності до тієї чи іншої категорії КІІ, можна визначити атрибут, що характеризує вміння долати захисні заходи та проникнення.

Розглянута модель активно застосовується експертами та дослідниками. Перспективним напрямом є використання методів машинного навчання, у тому числі глибокого навчання, для автоматизації процесів вилучення та ідентифікації відповідних методів і засобів, окремих етапів ланцюжків, унікальних ознак APT та інших функцій, які будуть включені в процес атрибуції. У пропонується розв'язання задач обробки великого потоку несортованих даних, які є первинними, і зниження кількості помилкових спрацьовувань, тобто інформаційних завад. Зловмисник - актор (порушник), який атакує жертву після аналізу своїх можливостей щодо реалізованих операцій над її інфраструктурою.

- *Можливості* уявляють собою характеристики, що описують інструменти та методи зловмисника, які застосовуються під час кібератаки.

- *Інфраструктура* здійснює опис зв'язки як фізичні так і логічні, які зловмисник використовує для реалізації можливостей з досягнення результату.
- *Жертва* уявляє собою мету, на яку здійснюється кібератака зловмисника.

Для розширення властивостей основних компонентів додатково присутні мета-характеристики або функції, що є часовою міткою, тобто початок події, кінець події, фаза, результат, напрямок, методологія та ресурси. Модель *Diamond* розширюється за допомогою мета-характеристик. Описані за замовчуванням мета-характеристики не є остаточними. Модель *Diamond* не обмежується перерахованими вище компонентами.

Розширена модель Diamond (*EDM*)

Розширену модель *Diamond* доповнено двома мета-характеристиками або ознаками, що відображають (1) застосовані порушником технології та (2) соціально-політичні мотиви. Технології встановлюють взаємозв'язок між інфраструктурою і можливостями, описуючи методи і засоби, що дають змогу інфраструктурі і можливостям ефективно взаємодіяти. Наприклад, якщо порушник застосовує систему доменних імен для адміністрування шкідливого рішення з метою здійснення командування і контролю над інфраструктурою жертви, тоді *EDM* є частиною технологій.

Взаємозв'язок між зловмисником і жертвою описує соціально - політична мета-характеристика. Вона характеризує основні потреби, прагнення та наміри порушника. Аналіз таких даних дає змогу виявити причину, через яку було обрано жертву, її цінність для зловмисника і як можна використати цей взаємозв'язок для протидії порушнику, як це представлено на рисунку 1.5.

Переміщаючись від однієї вершини до іншої, застосовуючи отримані відомості під час аналізу кібератаки, дослідники формують гіпотези. Спростування, доведення або зміна даних гіпотез у моделі називається аналітичним обертанням. Наявність встановлених моделлю компонентів дає

змогу зосередитися на конкретній вершині даної функції для цілеспрямованого ("*центрованого*") аналізу вторгнення.

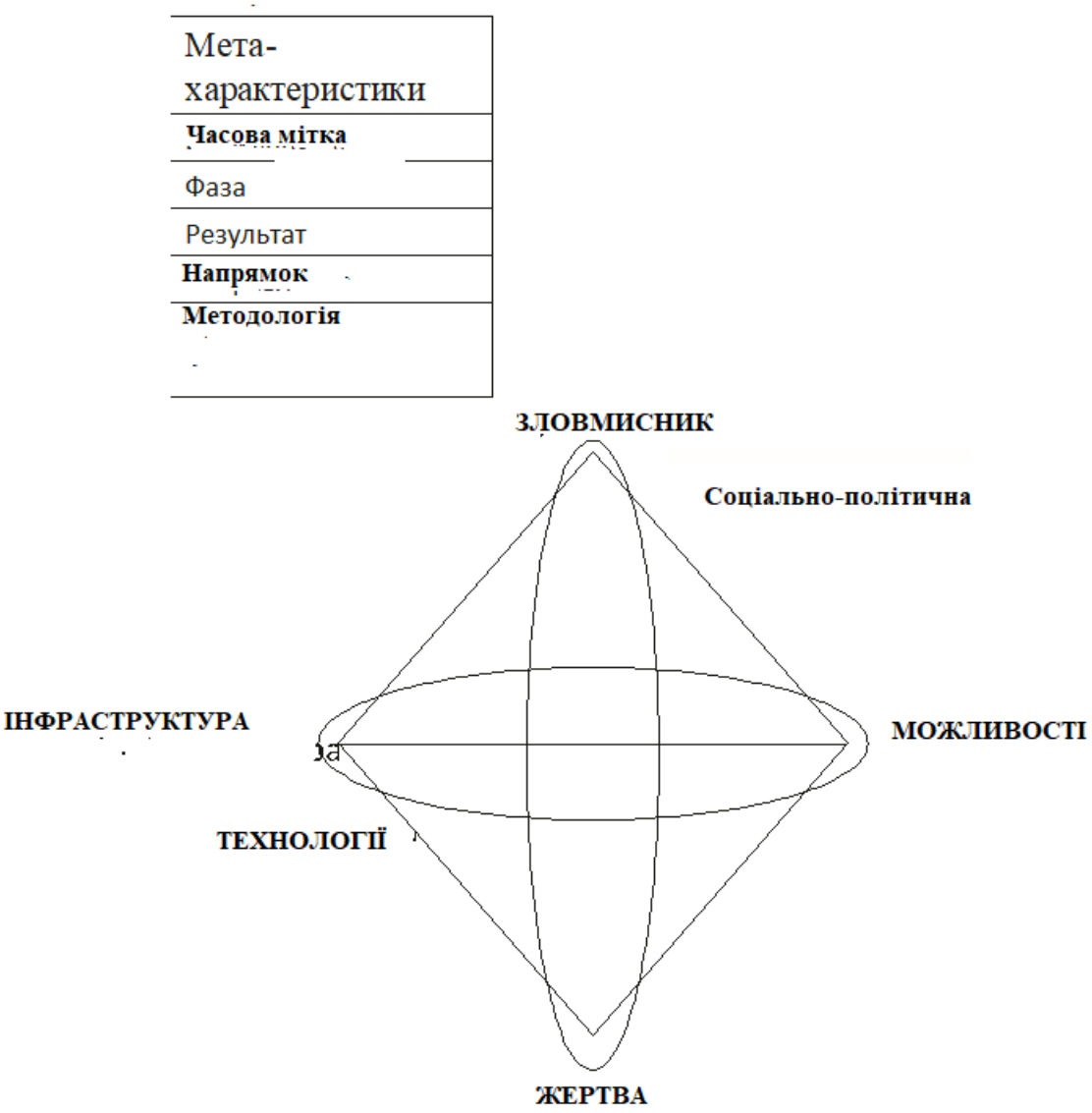

Рисунок 1.5. Розширена модель *Diamond*.

Таким чином, виконуючи аналіз з боку жертви, аналітики можуть зрозуміти, як саме сталася кібератака, виявити вразливі місця і скомпрометовану інфраструктуру, з боку інфраструктури - можливості порушників, дії, які здійснюються в інфраструктурі або над інфраструктурою) та, орієнтуючись на порушника, - сформувати область атакованих об'єктів, щоб визначити спеціалізацію порушника.

Відповідно до цієї моделі порушник виконує послідовні дії, які містять мінімум дві результативні фази для виконання поставленого завдання. Такі дії називаються потоком активності та мають причинно-наслідковий зв'язок. Потоки можуть проходити по вертикалі та горизонталі. Потік активності представлений у вигляді структурованого за фазами графа атак. Вершина є подією, а дуги (орієнтовані ребра) відображають причинно-наслідкові зв'язки між подіями.

На рисунку 1.6 представлено приклад потоку активності, що відображає дії порушників щодо жертв.

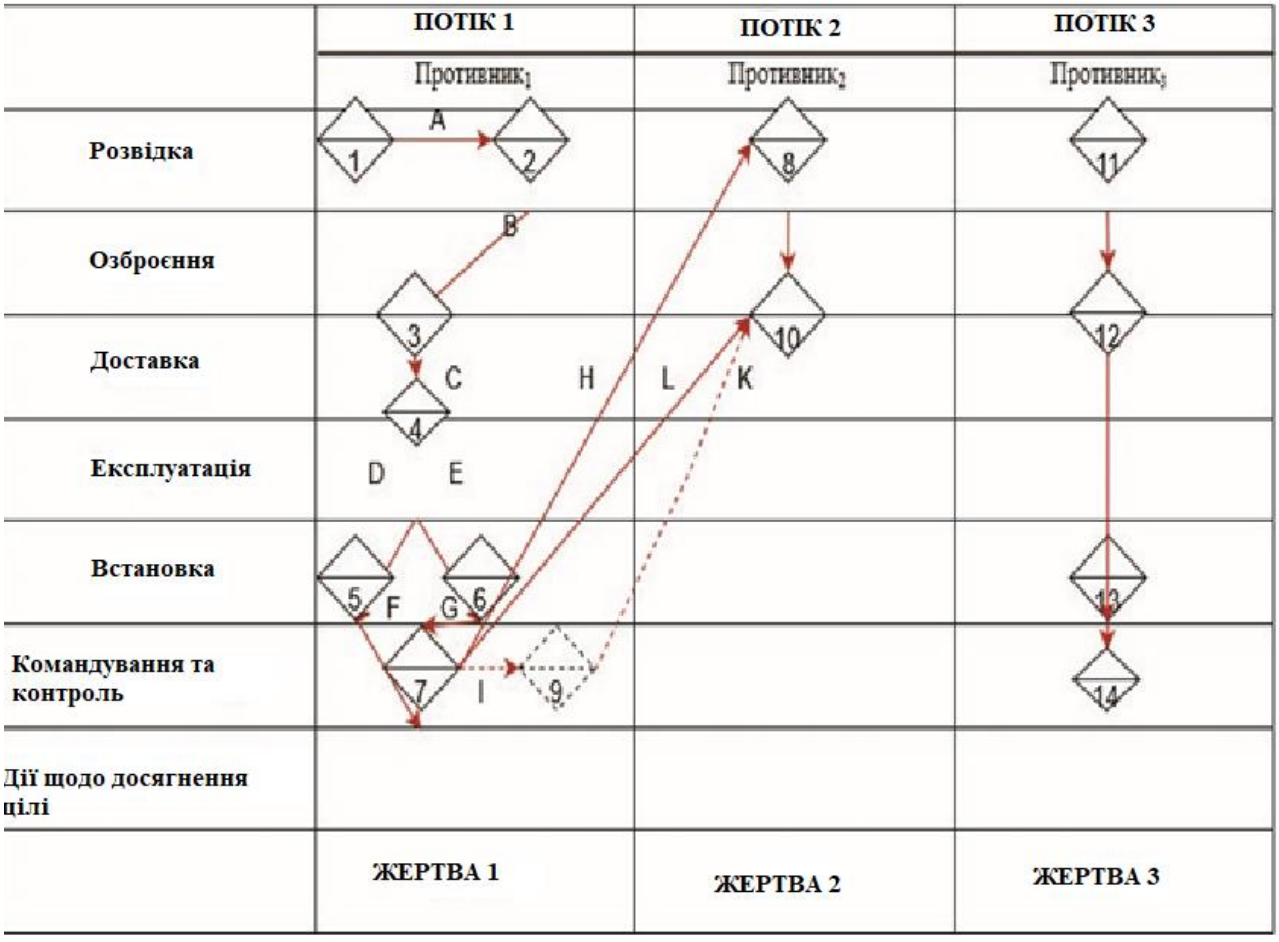

Рисунок 1.6. Потік активності.

Зв'язки, виділені пунктиром, позначають здатність аналітиків об'єднувати гіпотези. Такий підхід дає змогу заповнювати прогалини під час аналізу кібератаки. Під графи цих потоків називаються протиборчими процесами, які можуть бути корисними пізніше для групування і класифікації дій на основі процесу, а не окремих індикаторів.

Приклад опису значень потоку активності жертви № 3 наведено в таблиці 1.

Таблиця 1.1.

ДІЇ ПОТОКУ АКТИВНОСТІ ЗЛОВМИСНИКА

Події	Дуга	**ДІЇ ЗЛОВМИСНИКА**	**ІТОГ**
11	M	Сканирование веб-сервисов на наличие уязвимостей	Результат сканирования сообщает о наличии уязвимых веб-сервисов и возможности применения эксплойта
12	N	Подбор эксплойта Доставка эксплойта жертве по сети	Эксплойт найден Доставка осуществлена успешно
		Запуск эксплойта	Запуск осуществлен успешно
		Установка на уязвимый сервер жертвы средств удаленного администрирования	Установка завершена успешно
13	O	Соединение с компрометированным сервером	Получен доступ к средствам удалённого администрирования, сервер доступен для выполнения удаленных команд

Щоб спрогнозувати потенційний вектор атаки противника, у моделі об'єднуються потік активності та граф атак у граф активності-атаки, як це представлено на рисунку 1.7.Знання про дійсні вектори атак інтегруються в безліч гіпотетичних векторів для позначення потенційних або традиційних шляхів реалізації атаки в майбутньому.

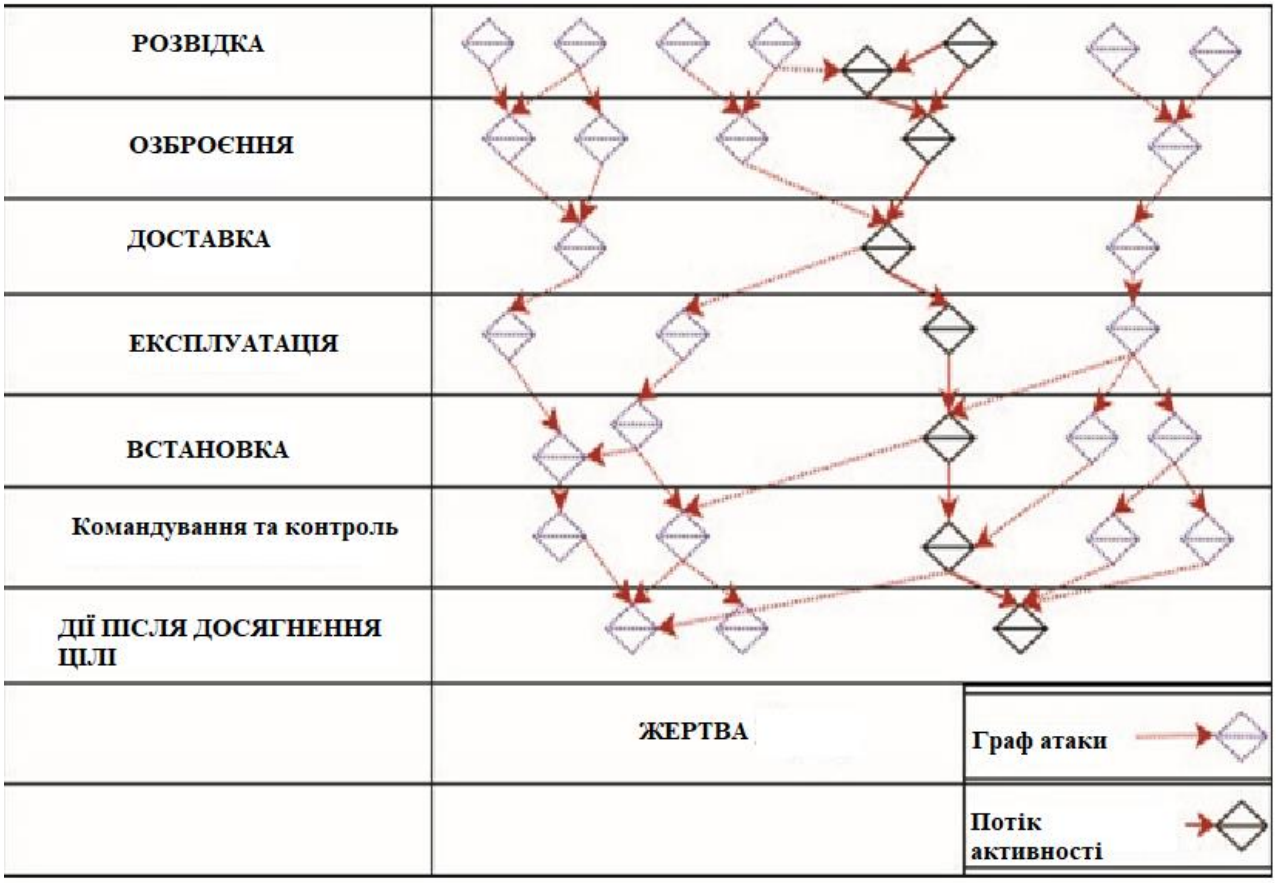

Рисунок 1.7. Граф активності - атаки

Для розв'язання завдань з атрибуції порушника, у моделі пропонується концепція групи дій. Схожі відомості про кібератаку (інфраструктуру, можливості, процеси і потоки) об'єднуються в групи загальних (схожих) шкідливих подій. На підставі таких даних формуються групи порушників. Групи можуть включати в себе підгрупи тощо. Концепція є гнучкою і може бути застосована для ідентифікації будь-якої групи порушників, зокрема . Процес формування групи дій, включає шість етапів:
1. *Постановка аналітичного завдання*. Визначається аналітичне завдання, яке необхідно вирішити за допомогою групи дій;

2. *Вибір метрик*. Визначається набір метрик (показників, характеристик), за якими вимірюється схожість між кібератаками.

3. *Створення групи*. Шляхом кластеризації схожих відомостей за заданими метриками формується група дій.

4. *Зростання групи*. Розширення групи дій за рахунок збагачення додатковими відомостями.

5. *Аналіз*. Група дій аналізується на предмет розв'язання і доповнення аналітичного завдання.

6. *Перевизначення*. Для підтримання груп дії в актуальному стані, проводиться їх перегляд на основі оновлених відомостей.

Однією з переваг цієї моделі є надання списку функцій, які мають бути присутніми в кожній події. Цей підхід підвищує ефективність моделі, оскільки дає змогу виявляти прогалини в знаннях про кібератаку і за допомогою безлічі гіпотез усувати недоліки в аналітичних відомостях. Модель встановлює основу для dkfcnbdjcntq протоколів обміну інформацією про кіберзагрози та управління знаннями. Модель може доповнюватися на певних рівнях іншими моделями. Наприклад, інтеграція з моделлю *UKC* дасть змогу поліпшити результати під час аналізу окремих етапів дій порушника. Модель може також використовуватися для аналізу вторгнень і класифікації подій у реальному часі на основі застосування аналітичного підходу та структурування даних про вже досліджених зловмисників. Можна зазначити, що модель має широкий потенціал для застосування для атрибуції порушників.

Модель MITRE ATT &CK

Модель ATT&CK , ще звана матрицею або базою знань, заснована на реальних подіях і містить інформацію про методи, методики та процедури, що застосовуються порушниками. Інформація в базі знань *MITRE ATT &CK* представлена у вигляді набору матриць.

Наведемо нижче основні компоненти моделі *MITRE ATT &CK* : тактики, процедури.

Тактики позначають проміжні або основні цілі порушника під час реалізації кібератаки. Кожна тактична категорія включає в себе техніки.

Техніки складають прийоми, що допомагають порушникам для досягнення основних цілей.

Інструментарій уявляє собою більш детальний опис на низькому рівні технік, що включає відомості про інструментарій.

Процедури реалізують конкретні випадки застосування технік і підтехнік. Формальний взаємозв'язок між окремими компонентами моделі можна відобразити у вигляді діаграми, як це представлено на рисунку 1.8.

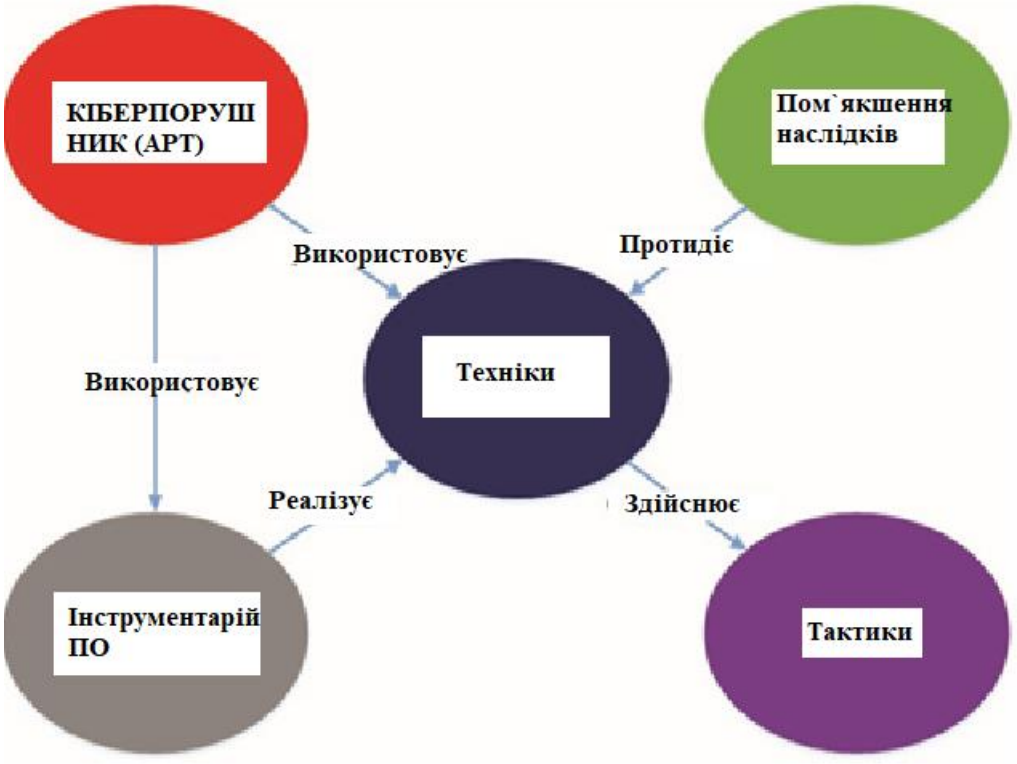

Рисунок 1.8. Взаємозв`язки моделі *MITRE ATT &CK*

Модель представлена у вигляді технологічних доменів і включає такі сфери застосування:

(1) *MITRE ATT &CK* уявляє собою корпоративний сегмент;

(2) *MITRE ATT &CK* застосовується для мобільних пристроїв;

(3) *MITRE ATT &CK* уявляють собою промислові системи керування, як-от автоматизовані системи керування технологічним виробництвом та системи диспетчеризації та збору даних .

У корпоративному сегменті на даний момент виділено чотирнадцять тактик:
- розвідка - порушники збирають корисну інформацію для планування і вдосконалення кібератаки;

- розвиток ресурсів - етап передбачає підготовку інфраструктури, необхідної для вторгнення, і розширення можливостей інструментарію;

- початковий доступ - порушниками здійснюється спроба здійснення доступу до інформаційних ресурсів цільового об'єкта; робиться спроба закріпитися в мережі жертви;
- реалізація - запуск шкідливого коду (реалізація інструментарію) на підконтрольному вузлі або системі; на даній стадії, атакуючі намагаються розширити свої можливості в інфраструктурі жертви;

- забезпечення постійної присутності - забезпечення тривалого доступу до скомпрометованого середовища на основі застосування методів, що дають змогу здійснювати стійкий доступ в умовах зміни скомпрометованого середовища;
- підвищення привілеїв - порушники здійснюють спроби розширити свої права, отримати вищі привілеї в цільовій системі;

- ухилення від захисту - порушники застосовують методи обходу засобів захисту і приховування своєї присутності в цільовій системі;

- доступ до облікових даних - маніпуляція обліковими даними користувачів, інформаційних систем, служб з метою отримання санкціонованого доступу до скомпрометованої інфраструктури жертви;

- виявлення - порушники здійснюють збір відомостей про інфраструктуру з метою реалізації кібератаки;

- бічний зсув - переміщення всередині скомпрометованої інфраструктури за рахунок інформаційних ресурсів жертви для досягнення основної мети;
- збір даних - порушники застосовують методи ідентифікації та агрегації конфіденційних даних у скомпрометованому середовищі для їх крадіжки, зміни або знищення;

- командування і контроль - порушники застосовують методики для забезпечення зв'язку та адміністрування керованої ними інфраструктури;
- ексфільтрація - вивантаження (викрадення) даних із цільового середовища;
- заподіяння шкоди - вплив на інфраструктуру жертви для реалізації мети атаки і приховування слідів або ускладнення протидії.

Для категоризації та опису дій порушників на ранніх стадіях життєвого циклу реалізації кібератаки, тактики "Розвідка і Розвиток ресурсів" класифіковані як підготовчий етап. Виділяється десять базових технік на етапі розвідки і сім технік на етапі підготовки ресурсів. Як додаткова деталізація і підвищення порівняльних характеристик дій порушників на початковому етапі *PRE Matrix* можна інтегрувати в модель *СКС*. На відміну від моделі *СКС*, у моделі *MITRE ATT &CK* тактики не утворюють послідовність, а передбачаються вибіркові дії порушників.

Модель *MITRE ATT &CK* містить у собі класифікацію відомих угруповань або окремих акторів, які відслідковуються державними і приватними організаціями у сфері кіберзлочинів. Відомості про них згруповані в окремий профіль і включають такі характеристики:

- назва угруповання;

- унікальний ідентифікатор (*id*);

- пов'язані угруповання (кібератаки);

- опис;

- застосовувані техніки та інструментарій.

Говорячи про КІІ, окремо варто виділити під модель *MITRE ATT & CK* для систем промислового управління *MITRE ATT & CK*. Саме індустріальні системи відповідають за технологічні процеси КІІ. Основний фокус зроблено на методах порушників, мета яких полягає в заподіянні шкоди промисловим системам та процесам. Відмінності від моделі для корпоративного сегмента є несуттєвими. Загалом виділено дванадцять тактик:

- початковий доступ;

- реалізація;

- забезпечення постійної присутності;

- підвищення привілеїв;

- ухилення;

- виявлення;

- бічне зміщення;

- збір даних;

- командування і контроль;

- придушення функції відгуку або функція заборони реагування, тобто дії порушників спрямовані на блокування функцій оповіщення оператора системи про інциденти безпеки, встановлених для технологічних процесів; відбувається маскування деструктивного впливу на систему через запобігання очікуваним сигналам тривоги на збої, критичні відхилення від заданих сценаріїв у роботі; на відміну від методів, що застосовуються на стадії "ухилення", прийоми придушення функції відгуку можуть бути більш інтрузивними, наприклад, активне блокування реакції

- порушення управління процесами - маніпуляція, порушення або відключення контрольованих фізичних процесів у цільовому середовищі; часто застосовується з тактикою "Придушення функції відгуку";

- заподіяння шкоди.

Матриця промислових систем пропонує базові визначення поведінки порушників у цьому середовищі. У своїй галузі проект є авторитетним і перспективним для застосування в системі атрибуції порушників під час цільових атак на об'єкти КІІ. З метою детального аналізу і підвищення якості атрибуції, можна розглянути або дослідити застосування матриці в поєднанні з вище розглянутими її компонентами і моделями аналізу вторгнень. За винятком традиційного призначення для моделювання загроз, пом'якшення наслідків, планування кібервторгнень. Модель *MITRE ATT&CK* може використовуватися як поведінкова модель порушників (*APT*) і описувати дії впродовж усього життєвого циклу кібератаки. На основі наявних профілів кіберугруповань модель *MITRE ATT&CK* дозволяє проводити атрибуцію *APT* методом класифікації отриманих даних за характерними для конкретних ознаками (*Сигнатурами*). Крім того, ця модель може виступати джерелом збагачення наявної бази профілювання *APT*.

1.3. Узагальнений аналіз підходів до реалізації методик та створенню автоматизованих систем атрибуції

КІІ зазнають багатовимірних кіберзагроз, у яких складно виокремити межі між інформаційними технологіями та промисловими системами - переміщаючись мережами, атакуючі використовують інформаційні технології для вибору й реалізації вектору атак на автоматизовані системи керування технологічними процесами. Отже, необхідно застосовувати комплексний (гібридний) підхід для аналізу та атрибуції цільових атак на КІІ.

Найважливішим елементом при виконанні атрибуції є збір необхідних даних. Дані, які збираються, обробляються й аналізуються для розуміння мотивів, цілей

і поведінки порушника. Застосовувані стандарти, наприклад, XML, JSON, CybOX/STIX, OpenIOC, IODEF, CAPEC і MAEC дають змогу детально описувати інциденти кібербезпеки. Загальноприйнятими протоколами обміну даних про загрози є TAXII і STIX. Їх використання робить обмін даними своєчасним і безпечним. Пропонований підхід CyberSANE спрямований на роботу з моделями аналізу вторгнень, здатними визначати приховані та непрямі вектори кібератак на цільову систему, зокрема атаки, що використовуються *APT* , програми-вимагачі та ботнети. Аналітика загроз ґрунтується на збиранні даних з відкритих джерел, соціальних мереж, спеціалізованих форумах, даркнеті тощо. Дані про порушників поділяються на три типи:

- тактичні - інформація технічного характеру, одержувана від різних індикаторів компрометації;
- операційні - відомості для формування профілю, наприклад, про тактики, техніки і процедури (ТТП). Спеціалізацію, можливості, географічну локацію тощо;
- стратегічні - дані про можливий збиток у разі деструктивного впливу на цільовий об'єкт.

Щоб забезпечити структурований формат даних, процес обробки інформації проходить кілька стадій, як це представлено на рисунку 1.9.

- планування процедур збору та обробки;

необхідних даних і процедур їхнього аналізу для автоматизованого або ручного виконання сценаріїв;

- збір і обробка даних - збір необхідної інформації, організація єдиного формату, видалення дублікатів даних. Обробка включає оперативний пошук і вилучення конкретних відомостей, кластеризація даних;

- підготовка - аналіз даних, виявлення недоліків у роботі алгоритмів, що застосовуються на ранніх етапах. Дослідження на предмет підозрілого або шкідливого змісту;

- поширення - передача даних про кіберзагрози, зокрема компоненту атрибуції, забезпечуючи збагачення інформацією з аналізу загроз.

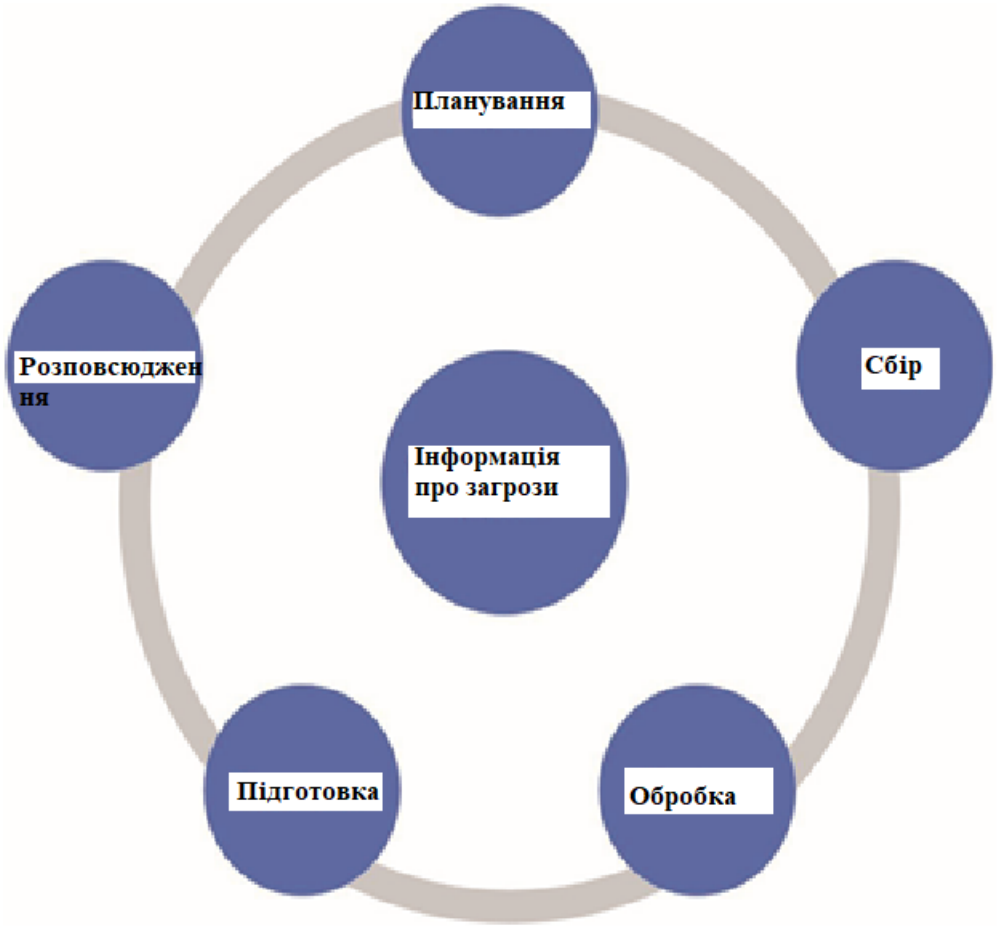

Рисунок 1.9. Цикл формування даних щодо кіберзагроз.

Використання аналітики загроз входить до складу більшості сучасних рішень з виявлення та атрибуції *APT*: Kaspersky Threat Intelligence Portal, IBM X-Force Exchange, Anomali ThreatStream, SolarWinds Security Event Manager, Palo Alto Networks Cortex XSOAR TIM тощо.

Цей підхід підтримує можливість автоматизації, оновлення в режимі реального часу, інтеграції з різними системами, застосування методів штучного інтелекту і машинного навчання.

Наявність стандартів опису загроз та протоколів обміну даними, дають змогу автоматизувати процес атрибуції. Зважаючи на брак підготовлених фахівців, автоматизація є пріоритетним напрямком у більшості організацій. Застосування методів машинного навчання дає змогу підвищити ефективність операцій атрибуції.

Широке застосування оновлень у режимі реального часу дає можливість своєчасно збагачувати структурованими даними базу профілів порушників (*APT*), підтримуючи її в актуальному стані.

Для підвищення ефективності процесів аналізу цільових кібератак і атрибуції важлива інтеграція систем атрибуції з *SIEM* -системами та іншими системами управління безпекою, даючи змогу аналізувати та корелювати інформацію з інших джерел.

Покращувати атрибуцію можна за рахунок інтеграції перспективних методикb. У аналітика кіберзагроз, яка заснована на правилах асоціативного аналізу даних, дає змогу ідентифікувати кібератаку, пов'язувати її з порушником, а також видаляти надлишкові відомості, не пов'язані з атрибуцією кібератаки. Можливість застосування штучного інтелекту і машинного навчання, підвищує процеси автоматизації та інтелектуалізації, загалом даючи змогу домогтися якісніших результатів під час атрибуції порушників, які здійснюють цільові атаки на КІІ. Перспективні алгоритми машинного навчання у сфері кібербезпеки, а також можливі вектори атак на інтелектуальні системи, що застосовують такі алгоритми, розглянуто в. Таксономію алгоритмів машинного навчання, які добре зарекомендували себе під час розв'язання цих завдань, представлено на рисунку 1.10. У великій кількості робіт, наприклад, виконано аналіз застосування методів глибокого навчання для виявлення кібератак, зокрема на КІІ, і розв'язання завдань атрибуції кіберпорушників.

Виявлення *APT* з використанням методів машинного навчання в деяких випадках дає високі результати. Наприклад, застосування варіантів штучної

імунної системи і рекурентних нейронних мереж для виявлення *APT* , показало, що запропоновані алгоритми забезпечують не тільки можливість виявлення, а й дають змогу провести атрибуцію *APT* з точністю від шестидесяти двох до дев`яносто дев`ти відсотків .

В даній роботі вдалося з високою точністю виявити *APT* у реальному часі та провести класифікацію кібератак. У роботі [4]

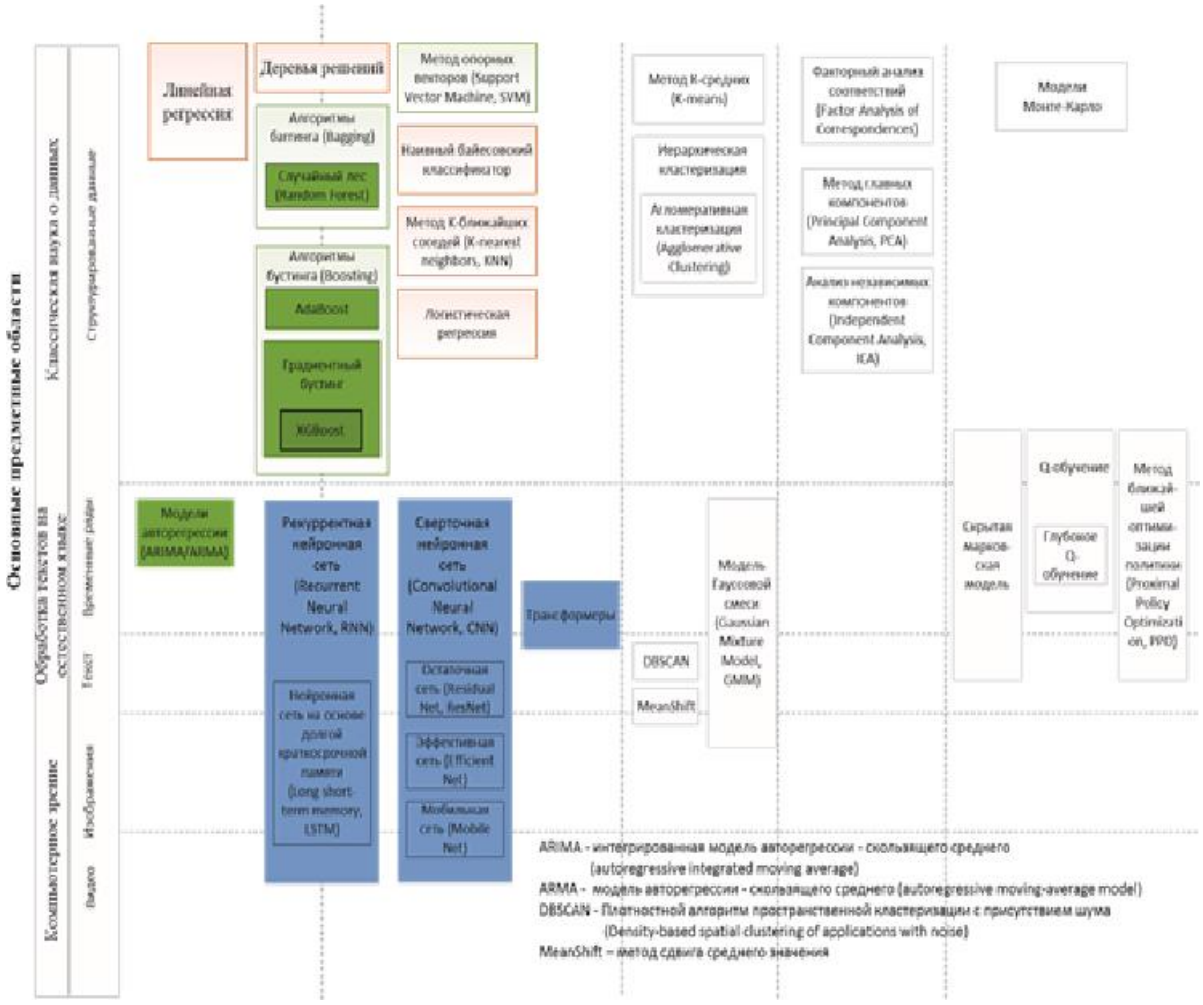

Рисунок 1.10. Таксономія алгоритмів машинного навчання.

Перспективні алгоритми машинного навчання у сфері кібербезпеки, а також можливі вектори атак на інтелектуальні системи, що застосовують такі алгоритми автоматизоване профілювання *APT* із застосуванням машинного навчання на основі шаблонів цільових атак дозволило забезпечити значення точності атрибуції від восьмидесяти трьох до дев`яносто чотирьох відсотків. Метод аргументованого міркування з доказами на технічному та соціальних рівнях для атрибуції кібератак представлено в роботі. Методику використання

технічних артефактів для виявлення хибних прапорів під час атрибуції цільових кібератак представлено в. Розглянемо нижче дві останні методики більш детально.

Методика і система атрибуції, засновані на аргументованому міркуванні (АМ).

Запропоновано методику і дослідницький прототип системи атрибуції на основі аргументації, які покликані допомогти дослідникам і фахівцям у процесі атрибуції кібератак.

Архітектура АМ складається з двох основних компонентів: компонента виведення або міркувань та бази знань, як це представлено на рисунку 1.11.

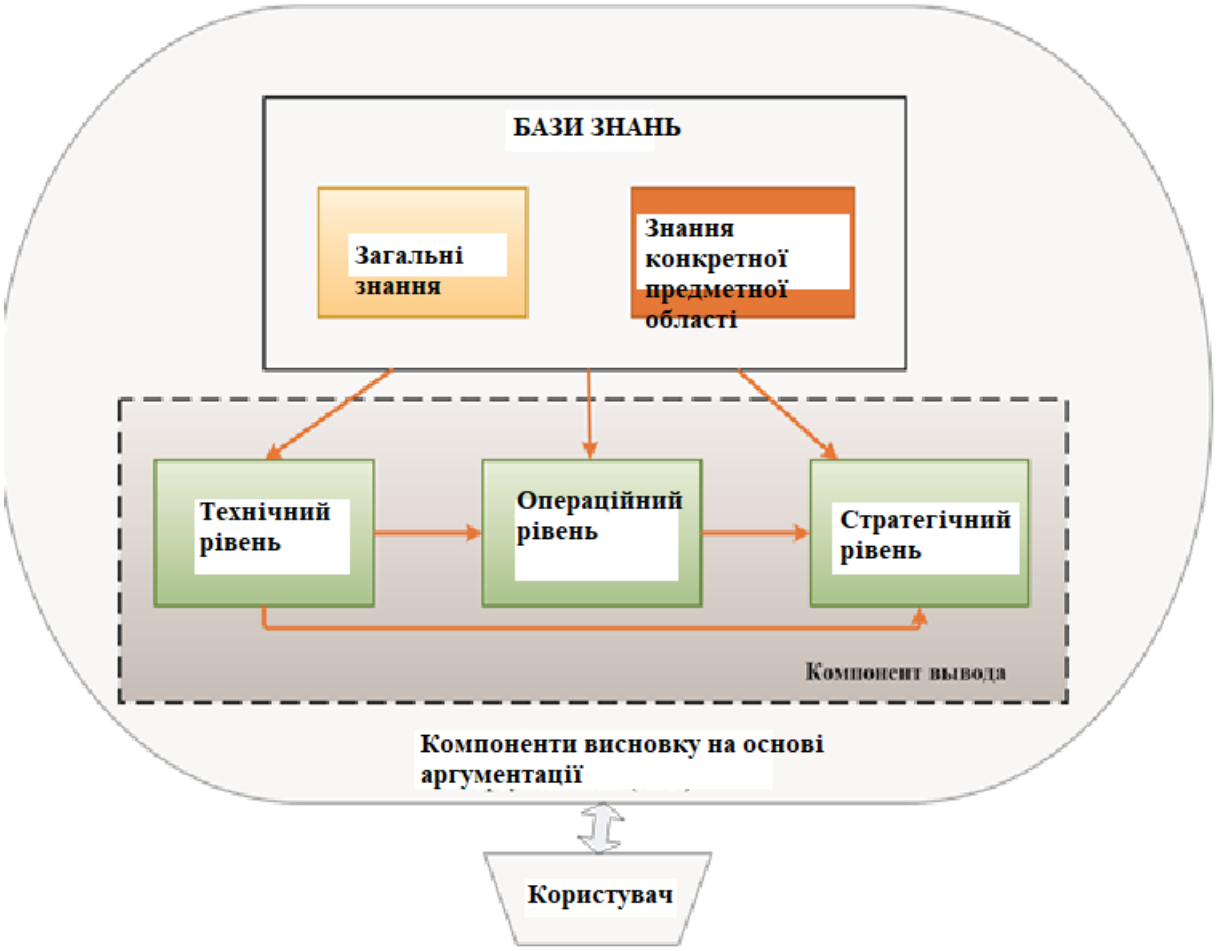

Рисунок 1.11. Компоненти аргументованого міркування

АМ використовує як технічні, так і соціальні докази, тобто свідчення, які отримані під час аналізу цільової кібератаки. Під час опрацювання вхідних даних

нетехнічного характеру використовується соціальна модель атрибуції, звана $Q-модель$. Докази і правила аргументованого міркування поділяються на три рівні: технічний, операційний і стратегічний. Комбінація інформації на цих рівнях спрямована на імітацію процесу розслідування кіберінцидентів з метою атрибуції кібератак.

Технічний рівень складається з правил, які стосуються доказів, отриманих унаслідок процесу розслідування інцидентів, пов'язаних із технічними аспектами реалізації атаки і тим, як її було здійснено. На цьому рівні визначають, наприклад, $IP-адресу$, з якої було здійснено атаку, час атаки, дані журналів, тип атаки, код, який використовували.

Операційний рівень складається з правил, що стосуються нетехнічних доказів, які стосуються соціальних аспектів. На цьому рівні виявляються, наприклад, відомості про те, де сталася кібератака, її можливі мотиви, необхідні можливості для її здійснення, політичний або економічний контекст даної цільової атаки.

Стратегічний рівень складається з правил, що стосуються ідентифікації кіберзлочинця.

Ґрунтуючись на реальних кібератаках із загальнодоступних джерел, АМ містить близько двохсот правил міркувань. Ці правила були перетворені на загальні правила аргументації і є одним з основних компонентів АМ. Взаємодіючи між собою на різних рівнях, правила дають змогу виконувати міркування, що лежать в основі атрибуції реальних кібератак. Вони також поділяються на три рівні: технічний, операційний і стратегічний. Знання поділяються на загальні знання і знання, що стосуються предметної області. Крім знань і даних про реальні атаки, у своїй роботі АМ також використовує фонові знання, що містять інформацію, яка не стосується конкретних випадків, тобто цільових кібератак. Застосування фонових знань допомагає мінімізувати помилки, пов'язані з людським фактором. Набір даних складається з фрагментів інформації, які використовуються правилами

виведення як попередні умови для відповіді на запити користувача або дослідника чи аналітика. Фонові знання АМ можуть бути оновлені та збагачені користувачем. Варто зазначити, що отримання осмислених висновків за допомогою застосування правил до знань залежить від правильності наданих знань.

Загальні знання складаються з інформації про характеристики країн, міжнародні відносини між ними та класифікацію організацій і промислових підприємств тощо. Ця інформація використовується разом із наданими доказами або свідченнями для проведення аналізу. До цієї категорії також належать дані про кіберпотенціал і можливості держав. Оцінюючи кіберпотенціал держави, можна обмежувати типи атак, які можуть входити до складу реалізованих цільових атак. Як джерела цієї інформації можуть слугувати, наприклад, дані групи глобального індексу кібербезпеки (Global Cybersecurity Index, GCI) і кіберможливості країн, що беруть участь у кібервійні . GCI являє собою складений індекс, що об'єднує двадцять п`ять показників в один еталонний показник для моніторингу та порівняння рівня зобов'язань держав щодо кібербезпеки. Виділяють три групи країн: провідні, ті, що розвиваються, і ті, що ініціюють. Крім того, на основі кіберможливостей у кібервійні деякі країни визначають як кібернаддержави, а саме США, КНР, Російська Федерація, Ізраїль, Велика Британія.

Знання предметної області складаються з інформації про відомі *APT*, окремі кіберугруповання та здійснені кібератаки. Цю інформацію здебільшого використовують на стратегічному та технічному рівнях. Відомі *APT* включають наступний набір атрибутів: назва або ідентифікатор; країна походження; країни/організації, на які кіберугруповання звертало увагу в минулому; шкідливе ПЗ або фрагменти шкідливого ПЗ які підозрювані або підтверджені, пов'язані з кіберугрупованням, а також відносини цього кіберугруповання з іншими суб'єктами, одними з яких є уряди. Ще одна важлива частина предметно-орієнтованих знань - схожість із минулими цільовими атаками. Наприклад, схожість зі шкідливою програмою, пов'язаною з конкретною *APT*, може

вказувати на те, що за кібератаку може відповідати те саме кіберугруповання. Отримані під час роботи АМ результати є аргументами для нових гіпотез дослідження кібератаки. Використання аргументованого підходу, що ґрунтується на уподобаннях та аргументованих міркуваннях , дає змогу АМ працювати із суперечливими доказами (гіпотезами) і заповнювати прогалини в знаннях, що виникають через неповноту даних.

Представлена в методика дозволяє здійснювати атрибуцію кіберпорушників інтерактивно, роблячи висновки прозоро для аналітиків. Незважаючи на здатність здійснювати атрибуцію і вибудовувати гіпотези, АМ сильно залежить від правильності наданих даних. Основна мета АМ - допомогти аналітику в процесі аналізу та надати корисну інформацію. Говорячи про перспективну систему атрибуції загалом, застосування методики міркування на основі аргументації може розглядатися як додатковий засіб автоматизації, підвищуючи швидкодію і точність процесу атрибуції кіберпорушника.

Висновки до розділу 1

1.Представлено аналіз актуальних моделей і методик, що використовуються для атрибуції порушників кібербезпеки під час реалізації цільових кібератак на об'єкти критичної інфраструктури.

2.Розглянутий клас загроз - цільові атаки на об'єкти КІІ, важливим підкласом яких є просунуті постійні загрози (*APT*), - вимагає багаторівневої класифікації на кожному етапі життєвого циклу кібератаки.

3.Застосування моделей "*ланцюжок кібервторгнень*" *CK* та *UKC* для опису етапів вторгнення, зіставлення індикаторів на різних фазах дії *APT* , виявлення закономірностей, що пов'язують окремі вторгнення з ширшими кампаніями з реалізації кібератак, дає змогу формувати дані для розуміння ітеративного характеру цільових атак і реалізації попередньої атрибуції порушника та цільових кібератак.

4.Моделі аналізу вторгнень *Diamond* та розширена ця модель дають змогу проводити високо ступеневу атрибуцію з урахуванням не тільки аналізу методик, методів та інструментарію реалізації кібератак, а й соціально-політичного контексту, вибудовуючи причинно-наслідкові зв'язки, а також підтримувати атрибуцію і виявлення цільових кібератак.

РОЗДІЛ 2 МЕТОДИКА ЗАСТОСУВАННЯ ТЕХНІЧНИХ ОБРАЗІВ ДЛЯ ВИЯВЛЕННЯ ХИБНИХ ПРАПОРІВ ПРИ АТРИБУЦІЇ ЦІЛЬОВИХ

Хибний прапор належить до тактики, яку застосовують кіберпорушники з метою приховати деструктивну активність під час цільової кібератаки або приховати свою присутність, звинувативши в реалізації кібератаки третю сторону. Пропонується модель атрибуції кіберпорушника із застосуванням технічних образів (*цифрового сліду*). Кожен деструктивний вплив здатен залишати після себе образи.

Передбачається, що аналізуючи *цифрового сліду* кіберпорушника, аналітики формують вхідні дані для процесу атрибуції кібератаки. Не зумівши виявити сфальсифіковані відомості, процес атрибуції піде за хибним сценарієм. На відміну від простого виявлення атак, атрибуція фокусується на зв'язку дій з дійовими особами. Тому важливим завданням стає визначення профілів акторів, які використовуються для порівняння дій з відомими профілями, зафіксованими у вже реалізованих *APT*. Знаючи, які сліди залишають зловмисники, можна визначити, які з них досить унікальні, а які можна легко підробити, заплутавши розслідування.

Відповідно до базової моделі "*ланцюжок кіберврторгнень*", у усі сліди (образи) кіберпорушників умовно поділяються на образи розвідки, озброєння, доставки, експлуатації, встановлення, управління та контролю, а також дій. До образів розвідки належать активні спроби сканування на мережевому рівні, дії з аналізу профілів на сайтах соціальних мереж, фішинг для збору інформації, атаки методом перебору паролів на зовнішні сервіси, наприклад, на веб-пошту

тощо.

Образи озброєння представляються даними про початкову техніку проникнення, зокрема наскільки складною вона була і скільки зусиль знадобилося кіберзловмиснику, чи використовували відомі вразливості та відомий інструментарій, чи було задіяно абсолютно нові, розроблені спеціально для досліджуваної кібератаки. Аналіз слідів озброєння дає змогу зібрати атрибути про можливості та ресурси зловмисників.

До образів доставки відносяться шляхи доставки шкідливого ПЗ (електронна пошта, миттєві повідомлення, інтернет-форум, SQL-ін'єкція, попутне завантаження тощо) і пов'язана з ними інформація (ідентифікатори, URL-адреси тощо).

Доповненням до цих моделей є велика база знань *MITRE ATT&CK*. Її застосування дає змогу здійснювати категоризацію і формування поведінкових ознак порушника (*APT*) і проводити поведінкову атрибуцію. Щоб мінімізувати фактори постійної еволюції *APT* і цільових атак, під час атрибуції необхідно застосовувати нові методи й алгоритми. Збагачення даних про кіберзагрози і кіберугруповання, методи штучного інтелекту і машинного навчання дають змогу перейти від ручних методик до автоматизованих і підвищити ефективність атрибуції під час цільових атак на КІІ. Представлені методики атрибуції на основі аргументації та використання технічних артефактів для виявлення хибних прапорів під час атрибуції є прикладами реалізованих наразі методики атрибуції кіберпорушників. У наступних роботах у межах концепції багаторівневої атрибуції, планується розвинути розроблені авторами цієї статті моделі, алгоритми та методики атрибуції, засновані на методах генерації та аналізу графів атак і методах машинного, зокрема глибокого навчання.

Хибний прапор належить до тактики, яку застосовують кіберпорушники з метою приховати деструктивну активність під час цільової кібератаки або приховати свою присутність, звинувативши в реалізації кібератаки третю сторону. Пропонується модель атрибуції кіберпорушника із застосуванням

технічних образів (*цифрового сліду*). Кожен деструктивний вплив здатен залишати після себе образ.

Передбачається, що аналізуючи цифровий слід кіберпорушника, аналітики формують вхідні дані для процесу атрибуції кібератаки. Не зумівши виявити сфальсифіковані відомості, процес атрибуції піде за хибним сценарієм. На відміну від простого виявлення атак, атрибуція фокусується на зв'язку дій з дійовими особами. Тому важливим завданням стає визначення профілів акторів, які використовуються для порівняння дій з відомими профілями, зафіксованими у вже реалізованих *APT*. Знаючи, які сліди залишають зловмисники, можна визначити, які з них досить унікальні, а які можна легко підробити, заплутавши розслідування.

Атрибуція відбувається шляхом зіставлення цих компонентів. Кожен компонент використовує технічні та соціально-політичні індикатори в поєднанні з компонентами *CAM – підходу*. Основна мета розслідування кібератаки - відповісти на запитання, хто жертва і чому, а також що сталося і як. Відповіді на ці запитання визначаються компонентами (1) віктимологія, (2) інфраструктура, (3) можливості та (4) мотивація.

Вони допомагають виявляти способи та методи реалізації конкретної кібератаки, необхідні можливості кіберпорушників, а також можливі "хибні прапори". Метою профілювання суб'єктів кіберзагроз є розробка профілів на основі минулих атак і пошук профілю, що відповідає висновкам на основі розслідування кібератак.

З технічного погляду процес атрибуції , який представлено полягає у виявленні джерела базових даних, збиранні аналітиками артефактів, вилученні корисних даних і формуванні відповіді на ключові запитання.

Запитання 1. Скільки зусиль (наприклад, потрібна велика команда, велика кількість робочих годин) потрібно кіберпорушнику для підробки артефакту, або зміни своїх дій для створення інших слідів?

Запитання 2. Скільки спеціальних знань потрібно, щоб маніпулювати відповідними артефактами і залишати лише незначні сліди?

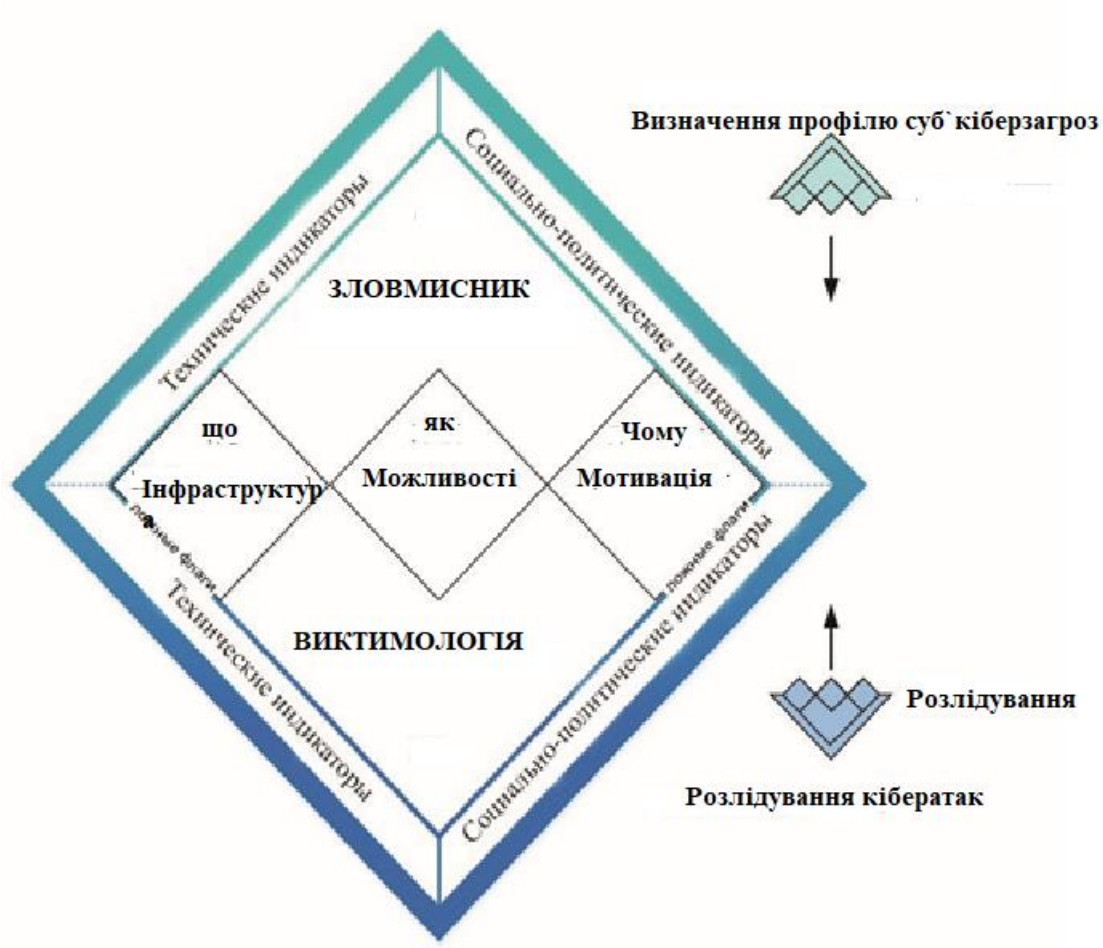

Рисунок 2.1. Моделі кібератрибуції

Запитання 3. Наскільки складно виявити сліди маніпуляцій або маскування?
Запитання 4. Наскільки унікальні та/або деталізовані потенційні сліди (образи)?
Запитання 5. Наскільки тісно пов'язані інші артефакти (важливо для створення цілісної картини)?

Для виконання атрибуції на першому етапі аналітики визначають, які джерела даних доступні. Як джерела даних може виступати розглянута матриця *MITRE ATT & CK*. Крім того, необхідно враховувати додаткові (переважно зовнішні) джерела даних, включно з каналами інформації про загрози, соціальними мережами та новинними стрічками. Щойно потенційно релевантні

джерела буде визначено, дослідники збирають артефакти, отримують інформацію вищого рівня та формулюють ключові запитання під час процесу атрибуції.

Заснована на ретельній оцінці технічних слідів, атрибуція спрямована на те, щоб краще зрозуміти точку зору зловмисника. У цьому процесі аналіз артефактів, розглянутих раніше, дає змогу дати відповіді на питання, що стосуються інфраструктури жертви (і будь-якої третьої сторони), можливостей актора і його конкретної мотивації. Багато окремих властивостей кібератаки можна сфальсифікувати і замаскувати, наприклад, IP-адресу приховують із використанням (ланцюжків) проксі-серверів або мережі TOR, зловмисники видають себе за інших, фальсифікують мовні налаштування, вводять неправдиві артефакти в коді і т. п. Проте, досить складно правильно зібрати всі ці цифрові сліди. Ретельна атрибуція має приділяти особливу увагу всій послідовності дій. Якщо якийсь один фактор має дивний вигляд або не вписується в очевидний сценарій, його необхідно перевірити ще раз, зробивши повторний аналіз. Слід зазначити, що "помилкові прапори" завжди присутні з таких причин:
- експлойти, що застосовуються кіберзлочинцями, містять перероблений код або використовувалися раніше і стали загальнодоступними;

- розробляється спеціалізоване ПЗ для імітації поведінки і збільшення складності атрибуції шкідливих програм;

- найчастіше експлойти і шкідливі програми купуються, а не розробляються;
- інструментарій для цільових кібератак можна взяти в оренду як послугу;
- на етапі "командування і контроль", шкідливе ПЗ використовує відому інфраструктуру (третіх осіб), яка не належить до операторів шкідливого ПЗ;
- застосовуються методи соціальної інженерії з метою спрямувати розслідування за хибним сценарієм;

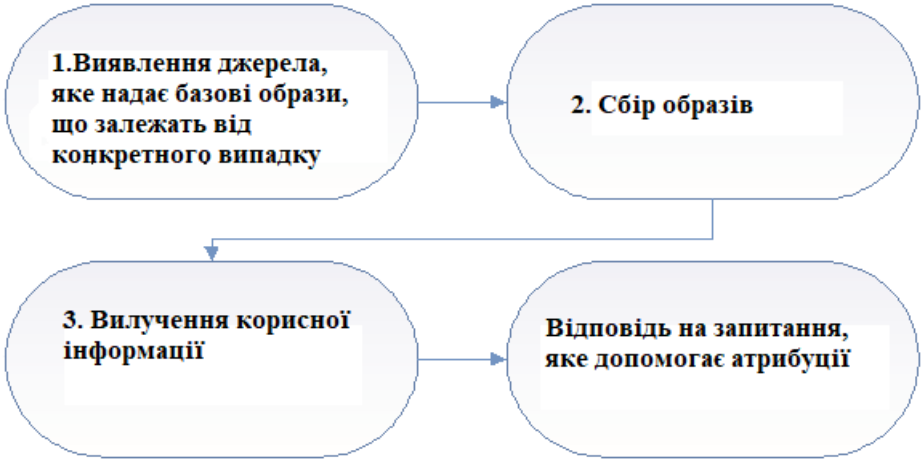

Рисунок 2.2. Спрощене представлення процесу атрибуції

- виконання дій з метою приховати сліди або ввести аналітиків в оману (наприклад, з використанням шифрування даних).

У перспективній системі атрибуції кіберпорушників під час реалізації ними цільових атак на об'єкти КІІ повинен бути присутнім компонент розпізнавання (пошуку) "хибних прапорів".

Висновок до розділу 2

1.Доповненням до розглянутих моделей є велика база знань *MITRE ATT & CK*. Її застосування дає змогу здійснювати категоризацію і формування поведінкових ознак порушника (*APT*) і проводити поведінкову атрибуцію.

2.Щоб мінімізувати фактори постійної еволюції *APT* і цільових атак, під час атрибуції необхідно застосовувати нові методи й алгоритми. Збагачення даних про кіберзагрози і кіберугруповання, методи штучного інтелекту і машинного навчання дають змогу перейти від ручних методик до автоматизованих і підвищити ефективність атрибуції під час цільових атак на КІІ.

3.Представлені методики атрибуції на основі аргументації та використання технічних артефактів для виявлення хибних прапорів під час атрибуції є прикладами реалізованих наразі методик атрибуції кіберпорушників.

ВИСНОВОК

1.На основі розгляду відкритих джерел у роботі представлено аналіз моделей і методик, які використовуються для атрибуції кіберзлочинців під час реалізації цільових атак, і які застосовуються як у наукових, так і в практичних проектах.

2.У роботі проведено аналіз нових моделей, що використовуються для атрибуції, які дають змогу здійснювати збір даних на тактико-технічному і соціо-політичному рівнях. Виокремлено основні показники кібератак і порушників, що проводяться, суттєві для реалізації процесів атрибуції.

3.Розглянуто порядок формування даних для профілювання кіберугруповань, а також можливості застосування розглянутих моделей і методик в інтересах побудови перспективної системи атрибуції кіберпорушника під час реалізації цільових атак на об'єкти критичної інформаційної інфраструктури.

4.Аналіз виконано за джерелами за двадцятирічний період, тим часом основні роботи, що розглядаються, були опубліковані за останні п'ять років. Аналіз не претендує на повноту, але робиться спроба охопити найбільш значущі дослідження.

5.Результат роботи полягає в тому, що представлена стаття є однією з перших вітчизняних праць, що надають розгорнутий аналіз досліджень, опублікованих за останні роки в галузі атрибуції порушників кібербезпеки.

6.Розглянуто такі моделі як "*ланцюжок кібератак*", "*уніфікований ланцюжок кібервторгнень*", базова та розширена моделі *Diamond* аналізу вторгнень , модель *ATT & CK* .

7.Наведено приклади методики атрибуції - аргументованого міркування з доказами на технічному та соціальних рівнях і використання технічних артефактів для виявлення хибних прапорів під час атрибуції. Крім того, перераховано тенденції в галузі використання сучасних рішень з виявлення та атрибуції атак на основі штучного інтелекту та машинного навчання.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ ТА ДЖЕРЕЛ

1. A. Suliman, M. K. Shankarapani, S. Mukkamala and A. H. Sung. RFID malware Cards and security devices for personal identification — Contactless proximity objects — Part 2: Radio frequency power and signal interface [Електронний ресурс] // ISO/IEC 14443-2:2020. – 2020. – Режим доступу до ресурсу: https://www.iso.org/standard/73597.html.

2. Guidelines for RFID-based Electronic Article Surveillance [Електронний ресурс]. – 2009. – Режим доступу до ресурсу: https://www.rfidjournal.com/gs1-releases-guidelines-for-rfid-based-electronic-article-surveillance.

3. IDTechEx: RFID System Frequencies. An overview of RFID frequencies for chip based tags. [Електронний ресурс]. – 2004. – Режим доступу до ресурсу: http://www.idtechex.com/.

4. L. Avanco, A. E. Guelfi, E. Pontes, A. A. A. Silva, S. T. Kofuji and F. Zhou. An effective intrusion detection approach for jamming attacks on RFID systems. International EURASIP Workshop on RFID Technology (EURFID); 2015; Rosenheim, Germany. p. 73–80.

5. Methodology for Evaluating Security in Commercial RFID Systems / T.M. Fernández-Caramés, P. Fraga-Lamas, M. Suárez- Albela, L. Castedo., 2017.

6. OpenPCD Reader [Електронний ресурс]. – 2016. – Режим доступу до ресурсу: https://www.meriac.com.

7. Vogt H. Efficient Object Identification with Passive RFID Tags / Harald Vogt. – Zürich: Department of Computer ScienceSwiss Federal Institute of Technology (ETH), 2002. – 98 с

8. Y. Fu, C. Zhang and J. Wang. A research on Denial of Service attack in passive RFID system. In: International Conference on Anti-Counterfeiting Security and Identification in Communication (ASID); 2010; Chengdu, China. p. 24–28.

9. Fragmentation attacks. In: International Symposium on Collaborative Technologies and Systems; 2008; Irvine, United States.

10. Агафьин С. С. LW-КРИПТОГРАФИЯ: ШИФРЫ ДЛЯ RFID-СИСТЕМ / С. С. Агафьин // Безопасность информационных технологий / С. С. Агафьин., 2011. – С. 30–33.

11. Гнатюк М. А. ДИФРАКЦИЯ ЭЛЕКТРОМАГНИТНОЙ ВОЛНЫ НА КАСКАДНОМ СОЕДИНЕНИИ ПРЯМОУГОЛЬНЫХ ВОЛНОВОДОВ / М. А. Гнатюк, В. М. Морозов, С. В. Марченко. // ХНУРЕ. – 2019. – №196. – С. 130–137.

12. Горбачов В. Е. ОБЗОР ПРОБЛЕМ БЕЗОПАСНОСТИ И ПРОЕКТИРОВАНИЯ ЗАЩИЩЕННЫХ ЭЛЕКТРОННЫХ СИСТЕМ / В. Е. Горбачов, К. Б. Абдулрахман. // ХНУРЕ. – 2017. – №191. – С. 113–119.

13. Горбенко І. Д. ДОСЛІДЖЕННЯ СТРУКТУРИ СПЕКТРІВ СИГНАЛОВ З ЛІНІЙНОЮ ЧАСТОТНОЮ МОДУЛЯЦІЄЮ / І. Д. Горбенко, О. А. Замула. // ХНУРЕ. – 2018. – №193. – С. 192–198.

14. Горбенко І. Д. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ПОМЕХОЗАЩИЩЕННОСТЬ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ В УСЛОВИЯХ РАЗЛИЧНЫХ ВНУТРЕННИХ И ВНЕШНИХ ВОЗДЕЙСТВИИ / І. Д. Горбенко, А. А. Замула, В. Л. Морозов. // ХНУРЕ. – 2017. – №189. – С. 5–14.

15. Горбенко Ю. І. УДОСКОНАЛЕНИЙ МЕХАНІЗМ ОДНОРАЗОВИХ КЛЮЧІВ ДЛЯ ПОСТКВАНТОВОГО ПЕРІОДУ НА ОСНОВІ ГЕШ-ФУНКЦІЙ [Електронний ресурс] / Ю. І. Горбенко, К. В. Ісірова // ХНУРЕ. – 2017. – Режим доступу до ресурсу: https://nure.ua/wp content/uploads/2017/Scientific_editions/191/5.pdf.

16. Описание процесса радиочастотной идентификации [Електронний ресурс] – Режим доступу до ресурсу: http://asupro.com/gps-gsm/meansidentification/reference/description-process-rfid.html.

17. Сальников Д. С. МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ДЛЯ БЕСПРОВОДНЫХ СИСТЕМ СВЯЗИ МИЛЛИМЕТРОВОГО ДИАПАЗОНА ВОЛН / Д. С. Сальников, А. І. Цопа. // ХНУРЕ. – 2018. – №192. – С. 140–148.

18. Шарфельд Т. Системы RFID низкой стоимости / Т. Шарфельд. – Москва, 2006. – 197 с.