## MATHEMATICAL AND COMPUTER MODELING

DOI 10.20535/2411-1031.2023.11.2.293768
УДК 004.056.53:621.391

ІГОР ЯКОВІВ

# МОДЕЛЬ ЧОТИРЬОХ ІНФОРМАЦІЙНИХ СЕРЕДОВИЩ КІБЕРАТАКИ

Основою функціонування сучасної інфраструктури кіберзахисту корпоративної інформаційної системи є процедура порівняння поточних подій в комп'ютерному середовищі з індикатором події безпеки. У разі збігу індикатора з відповідною подією формується інформація безпеки про цю подію. Вона передається для аналізу на засоби системи керування подіями та інформацією безпеки SIEM. За результатами аналізу приймається рішення про наявність інциденту кібербезпеки. На наступному етапі приймається та впроваджується рішення про відповідь на інцидент, що відновлює стан кібербезпеки. Обов'язковою умовою ефективної роботи інфраструктури кіберзахисту є наявність знань про можливі кіберзагрози та відповідні ознаки (індикатори) подій безпеки на технічному рівні комп'ютерних систем.

За формування ознак подій безпеки відповідає розвідка кіберзагроз (CTI). В умовах масштабного застосування звичайних повторюваних кібератак основною функцією CTI було визначення простих технічних ознак, які мають назву індикаторів компрометації (IOCs). В якості таких IOCs використовуються бітові послідовності (сигнатури).

В умовах широкомасштабного застосування складних кібератак актуальним стає завдання розробки таких карт прогнозування APT атак, що дозволяють формувати шаблони ознак подій безпеки (security event attributes pattern, SEAP) для автоматизованого детектування комп'ютерними засобами інфраструктури кіберзахисту.

Стаття присвячена розробці моделі, яка за допомогою атрибутивно-трансфертного підходу до сутності інформації, дозволяє формалізувати процеси кіберзахисту. Модель візуально деталізує та поєднує події, що розкривають сутність підготовки та реалізації APT атаки, процеси захисту від неї та завдання розвідки кіберзагроз щодо визначення конкретних даних для засобів ефективної інфраструктури кіберзахисту. Рівень деталізації моделі дозволяє застосовувати відомі математичні конструкції для опису подій та інформації безпеки. Такий підхід спрощує формування алгоритмів для засобів автоматизації процесів кіберзахисту.

**Ключові слова:** природа інформації, ментальне інформаційне середовище, комп'ютерне інформаційне середовище, інфраструктура кіберзахисту, проактивна стратегія захисту, розвідка кіберзагроз, SIEM, IDS/IPS, прогнозування APT, індикатори компрометації, шаблон подій безпеки, цикл керування кібербезпекою.

**Постановка проблеми.** Основою функціонування інфраструктури кіберзахисту корпоративної інформаційної системи є процедура порівняння поточних подій в комп'ютерному середовищі з індикатором події безпеки (security event). У разі збігу індикатора з подією формується інформація безпеки (security information) про цю подію, яка передається для аналізу на засоби системи управління подіями та інформацією безпеки SIEM (Security Information and Event Management). За результатами аналізу приймається рішення про наявність інциденту кібербезпеки. На наступному етапі кіберзахисту приймається та впроваджується рішення про відповідь на інцидент, яке відновлює стан кібербезпеки. Таким чином, обов'язковою умовою ефективної роботи інфраструктури кіберзахисту є наявність знань про можливі кіберзагрози та відповідні ознаки (індикатори) подій безпеки на технічному рівні комп'ютерних систем.

За формування ознак подій безпеки відповідає розвідка кіберзагроз (Cyber Threat Intelligence, CTI), або просто – розвідка загроз (Threat Intelligence, TI). В умовах масштабного застосування звичайних повторюваних кібератак основною функцією CTI було визначення простих технічних ознак, які мають назву індикаторів компрометації (Indicators Of Compromise, IOC). В якості таких IOCs використовуються бітові послідовності (сигнатури). Наприклад, IP-адреси хостів зловмисника, що реалізують DDOS атаку. Хеш-образ MD5 шкідливого файлу також є прикладом простого індикатору компрометації. Застосування таких простих IOCs ефективно в рамках реалізації реактивної стратегії кіберзахисту. Всі IOCs визначаються тільки за результатами аналізу зареєстрованих атак та потім швидко розповсюджуються в середовищі спільноти кіберзахисників.

Широкомасштабне застосування проти критичної інфраструктури складних кібератак типу APT (Advanced Persistent Threat, вдосконала стійка загроза або цільова загроза), відкрило новий етап розвитку CTI. Характерним для APTs є:

– атака представляє складний набір взаємозв'язаних за часом і простором дій зловмисника в комп'ютерному середовищі жертви. Окремо ці дії можуть не викликати підозр;

– цільова акція атаки в кіберсегменті об'єкта готується тривалий час (від декількох місяців до року і більше);

– сукупність дій зловмисника - це ланцюжок тактик, виконання яких дозволяє досягти мети атаки. Незважаючи на різноманітність засобів, що використовуються в APTs, набір більшості тактик та їх сутності залишаються постійними;

– як правило, таки атаки здійснюються тільки один раз на конкретний об'єкт (атака 0-дня), що ускладнює захист на основі простих IOCs.

В цих умовах актуальною стає проактивна (попереджувальна) стратегія кіберзахисту на основі переходу CTI до парадигми прогнозування можливих APTs на конкретну інформаційну систему (ІС) та формування відповідних складних наборів ознак подій безпеки для їх виявлення ще до кінця реалізації останнього етапу атаки. Стримуючим фактором розвитку у цьому напрямку є комплекс семантичних невизначеностей стосовно базових аспектів функціонування CTI. Основні з них:

– сутність та цілі CTI;
– складові та механізми реалізації;
– класифікація видів CTI;
– об'єкти та суб'єкти CTI.

Стаття присвячена розробці моделі, що за допомогою засобів формалізації на основі застосування атрибутивно-трансфертного підходу до сутності інформації дозволяє уточнити сенс завдань CTI щодо прогнозування APT атак. Така модель необхідна як для пояснення сутності прогнозування можливих APTs, так і для методів формування відповідних наборів (шаблонів) ознак подій безпеки, що можливо застосовувати комп'ютерними засобами інфраструктури кіберзахисту.

**Аналіз останніх досліджень і публікацій.** Можливо зустріти багато різних визначень терміну розвідка кіберзагроз, які пов'язуються з інформацією, даними або знаннями про різни аспекти діяльності у сфері кіберзахисту. Це приводить до значної невизначеності відносно сенсу організації процесів розвідки як корпоративної CTI, так і процесів ефективної кооперації спільноти кіберзахисників. Розглянемо деякі, найбільш розповсюджені, приклади.

Дослідницька компанія Gartner дає наступне визначення [1]:

*Розвідка про загрози – це знання, засновані на доказах, включаючи контекст, механізми, показники, наслідки та корисні поради, про існуючу або виникаючу загрозу чи небезпеку для активів, які можна використовувати для прийняття рішень щодо реакції суб'єкта. до цієї загрози чи небезпеки.*

Відома фірма IBM дає наступне тлумачення [3]:

*Розвідка про загрози, яку також називають «розвідкою про кіберзагрози» (cyber threat intelligence, CTI) або «розвідкою про загрози» (threat intel, TI ) – це дані, що містять докладні відомості про загрози кібербезпеці, спрямовані на організацію. Розвідка про загрози допомагає командам безпеки бути більш проактивними, дозволяючи їм вживати ефективних*

*дій на основі даних, щоб запобігти кібератакам до того, як вони відбудуться. Це також може допомогти організації краще виявляти поточні атаки та реагувати на них.*

Національний інститут стандартів і технологій (NIST) США пропонує свій варіант [4]:

*Розвідка про загрози – це інформація про загрози, яка була зібрана, перетворена, проаналізована, інтерпретована або збагачена, щоб забезпечити необхідний контекст для процесів прийняття рішень*.

Фірма VMware, яка виробляє спеціалізовані засоби для CTI, надає більш детальне визначення [5]:

*Threat Intelligence – це заснована на фактах інформація про кібератаки, яку організовують і аналізують експерти з кібербезпеки. Ця інформація може включати:*

- *механізми нападу;*
- *порядок визначення факту атаки;*
- *як різні типи атак можуть вплинути на бізнес;*
- *орієнтовані на дії поради щодо захисту від атак.*

Всі ці визначення та багато інших подібних мають загальний характер та потребують багато уточнень, що необхідні для організації ефективної корпоративної служби CTI. До засобів такого уточнення можна віднести:

- класифікацію по видам CTI;
- набори вимог до розвідувального продукту;
- моделі поведінки зловмисників та захисників;
- способи прогнозування APTs, які дозволяють формувати таки шаблоні ознак подій безпеки, які можливо застосовувати комп'ютерними засобами інфраструктури кіберзахисту.

Розглянемо ці аспекти послідовно.

Класифікація CTI. Широко розповсюджена наступна класифікація за видами корпоративної CTI [5]:

- *стратегічна CTI*: стратегічна розвідка про загрози – це інформація високого рівня, яка ставить загрозу в контекст. Це нетехнічна інформація, яку організація може представити раді директорів. Прикладом стратегічної розвідки про загрози є аналіз ризиків того, як бізнес-рішення може зробити організацію вразливою до кібератак;
- *оперативна CTI*: оперативна розвідка про загрози – це збір інформації, яку IT-відділ може використовувати як частину активного керування загрозами для вжиття заходів проти конкретної атаки. Це інформація про намір атаки, а також характер і час атаки. В ідеалі ця інформація збирається безпосередньо від зловмисників, що ускладнює її отримання;
- *тактична CTI*: тактичний аналіз загроз включає деталі того, як загрози здійснюються та можливі заходи захисту від них, включаючи вектори атак, інструменти та інфраструктуру, які використовують зловмисники, типи бізнесу або технології, на які спрямовано напад, і стратегії уникнення. Це також допомагає організації зрозуміти, наскільки ймовірно вона стане мішенню для різних типів атак. Експерти з кібербезпеки використовують тактичну інформацію, щоб приймати обґрунтовані рішення щодо контролю безпеки та керування захистом;
- *технічна CTI*: збір даних про технічні характеристики процесів в комп'ютерних системах, які є конкретними доказами того, що відбувається атака. Такими характеристиками, наприклад, можуть бути ідентифікатори шкідливих додатків фішингових повідомлень електронної, IP-адреси інфраструктури C2 або артефакти з відомих зразків шкідливого програмного забезпечення.

Вимоги до розвідувального продукту. Типовим прикладом рівня якості розвідувального продукту є наступні вимоги [5]:

- *достовірність (на основі доказів)*: щоб будь-який розвідувальний продукт був корисним, його спочатку потрібно отримати за допомогою належних методів збору доказів. Таким чином, аналітики, які покладаються на нього, можуть бути впевнені в його достовірності;
- *корисність*: щоб розвідка загроз мала позитивний вплив на результат інциденту безпеки або стан безпеки організації, вона повинна мати певну корисність. Розвідувальні дані

повинні надати ясність з точки зору контексту та даних про конкретну поведінку або методи, щоб визначити, чи оцінює аналітик інцидент у порівнянні з іншими інцидентами подібного характеру.

– *можливість практичного використання*: розвідувальні дані повинні стимулювати конкретні дії щодо покращення стану безпеки відносно кіберзагроз, з якими найбільш ймовірно зіткнеться організація.

Моделі поведінки зловмисників та захисників. Для прогнозування загроз та захисту від них в рамках CTI широко застосовуються моделі різного рівня складності від загального вербального та графічного опису до рівня математичної інтерпретації дій. Найбільш затребуваними є моделі, в яких математична інтерпретація супроводжується набором правил, які пов'язують дані в журналах подій з елементами математичних конструкцій.

На рівні загального опису найбільш відомі наступні моделі процесів атаки та захисту.

Діамантова модель (Diamond Model, DM) [6], що за допомогою схеми діаманта (рис.1) візуально поєднує основні аспекти загрози.

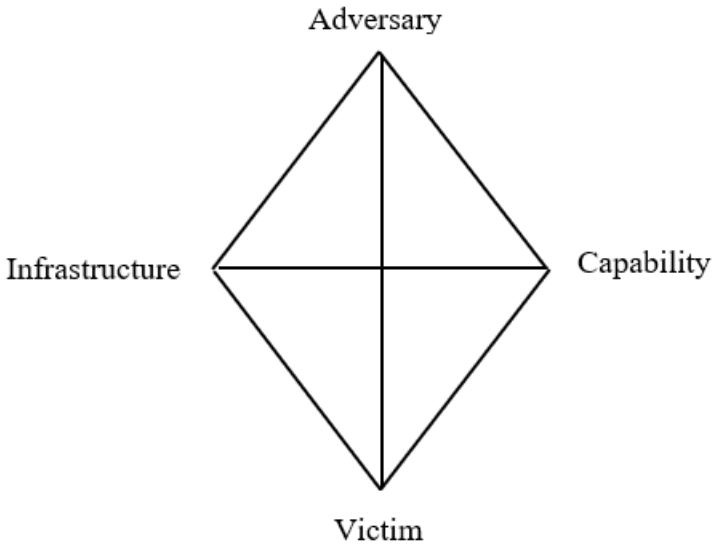


Рисунок 1 – Діамантова модель (Diamond Model

В моделі відображаються наступні сутності:

– *Adversary* (Противник) – це будь-хто, хто прагне скомпрометувати ресурси інформаційної системи, щоб просуватись у напрямку досягнення зловмисних цілей. Противником може бути зловмисник із внутрішнього або зовнішнього середовища системи, групи осіб або, навіть, організації;

– *Victim* (Жертва) – це об’єкти, що є ціллю втручання (окремі особи, групи осіб, організації, або окремі ресурси інформаційної системи (наприклад, електронна адреса, домен або база даних);

– *Infrastructure* (Інфраструктура) – це сукупність складових IT-середовища, що використовують хакери для реалізації своїх спроможностей в напрямку досягнення цілі. . Діапазон складових може бути від простих складових (доменні імена, заголовки IP-пакетів, IP-порти, облікові записи) до обчислювальних процесів та окремих пристроїв (USB-пристрої, комутатори, маршрутизатори, проміжні сервери зловмисного програмного забезпечення тощо);

– *Capability* (Спроможність) – це набір засобів/інструментів та заходів / технік, які застосовуються нападником для реалізації загрози та/або захисником для попередження загрози.

Схема у вигляді діаманта (ромба) візуально формує 4-мірний простір, в рамках якого можливо формувати прогнози про загрози та відповідні заходи безпеки. Прогнозування може бути з різної ступеню деталізації. Недолік моделі – відсутні доступні пояснення яким чином

можливо перейти від вербального опису до опису на основі технічних характеристик, що можуть «зрозуміти» комп'ютерним пристроям системи кіберзахисту.

Наступна відома модель загального опису – Ланцюжок кіберзнищення (Cyber Kill Chain, CKC). Запропонована трьома фахівцями корпорації Lockheed Martin [7]. Вона представляє дії зловмисника в рамках APT у вигляді послідовності етапів (рис. 2).

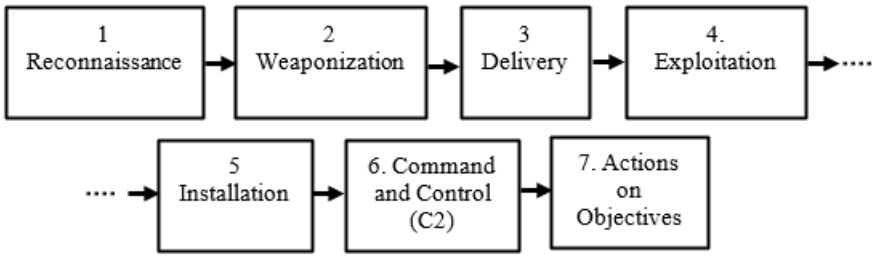


Рисунок 2 – Ланцюжок кіберзнищення (Cyber Kill Chain, CKC)

Сутність цих етапів ланцюжка знищення є така:

1. *Розвідка* (Reconnaissance) – дослідження, ідентифікація та вибір цілей, збір та аналіз інформації про жертву з відкритих джерел (веб-сайти організацій, відомості про організацію з Інтернет, матеріали конференцій, списки розсилки для адрес електронної пошти, соціальні мережі, інше).

2. *Озброєння* (Weaponization) – розробка стратегії атаки та комплексу необхідних засобів (зброї), що поєднує в собі засоби віддаленого доступу, необхідне для атаки програмне забезпечення та засоби автоматизованої активації цього програмного забезпечення. Відомі приклади таких засобів - файли даних клієнтських програм, такі як Adobe Portable Document Format (PDF) або документи Microsoft Office з активованими макросами.

3. *Доставка* (Delivery) – передача (проникнення) зброї в комп'ютерне середовище цільової організації. Три найпоширеніші вектори доставки озброєння учасниками APT – це вкладення електронної пошти, веб-сайти та змінні носії USB.

4. *Експлуатація* (Exploitation) – після того, як зброя доставлена, починається експлуатація вразливостей комп'ютерного середовища цільової організації. Найчастіше експлуатація націлена на вразливість програми або операційної системи, але вона також може простіше використовувати вразливості самих користувачів (фишинг) або використовувати функцію операційної системи, яка дозволяє автоматично виконувати зловмисний код.

5. *Встановлення* (Installation) – встановлення несанкціонованого каналу віддаленого доступу (бекдору) в систему-жертву, що дозволяє зловмиснику підтримувати стійкість у середовищі.

6. *Командування та керування* (Command and Control, C2) – за допомогою несанкціонованого каналу управління (бекдору) у реальному часі забезпечується дистанційне керування зловмисним програмним забезпеченням та/або функціями операційних систем в кіберсегменті жертви.

7. *Дії щодо цілей* або *цільова акція* (Actions on Objectives) – після проходження перших шести підготовчих етапів (тактик), зловмисники можуть вживати заходів для досягнення своїх стратегічних цілей. Як правило, це є викрадання даних, яке передбачає збір, шифрування та вилучення інформації з середовища жертви; порушення цілісності даних або їх доступності; також стратегічною ціллю може бути порушення роботи промислових об'єктів.

Модель дозволяє прогнозувати можливі APT атаки на ресурси корпоративної інформаційної системи шляхом вербального опису. Недолік цієї моделі – також відсутні доступні пояснення про перехід від вербального опису до опису, що зможуть «зрозуміти» комп'ютерні пристрої інфраструктури кіберзахисту.

Існує багато інтерпретацій цієї моделі, що відрізняються ступеню деталізації, межами та відмінностями змісту етапів. Широке розповсюдження знайшла інтерпретація корпорації Mitre [8], що використовує CKC для структурування знань про тактики та прийоми противника, що засновані на реальних спостереженнях. База знань (фреймворк) MITRE

ATT&CK дозволяє детально прогнозувати поведінку зловмисника за допомогою широко відомого концепту як тактики, техніки та процедури (Tactics, Techniques, Procedures, далі - TTPs).

1. *Тактика* (TA) – це проміжна технічна ціль супротивника, причина виконання дії та те, чого він намагається досягти. Кожна тактика прив'язана до етапу CKC. Досягнення стратегічної цілі реалізується через сукупність досягнення тактичних цілей. Наприклад, зловмисник може захотіти отримати облікові дані, щоб отримати доступ до цільової мережі.

2. *Техніки* (прийоми, T) представляють собою набір заходів, за допомогою яких противник досягає тактичної мети. Наприклад, зловмисник може попередньо скинути облікові дані, щоб потім отримати доступ до облікових даних.

3. *Підтехніки* – це різні варіанти технік з більш детальним описом. Не всі техніки мають підтехніки.

4. *Процедури* (P) – це набір необхідних засобів та ресурсів, що дозволяє реалізувати техніки (підтехніки).

В рамках MITRE ATT&CK всі техніки, підтехніки та процедури зв'язані з конкретною тактикою (етапом атаки). Кожна тактика, техніка та підтехніка мають унікальні ідентифікатори (ID). Наприклад, в рамках тактики *Reconnaissance* (Розвідка, ID: TA0043) може бути застосовано 9 технік, одна з яких – *Активне Сканування* (Active Scanning, ID: T1595). В свою чергу, техніка T1595 має три підтехніки T1595: 001; 002; 003. З цією технікою також пов'язані рекомендації щодо пом'якшення наслідків загрози (Mitigations, ID: M1056) та опис способів детектування техніки (Detection, ID: DS0029). Крім того, для кожної техніки додаються посилання на джерела (References), що на основі аналізу реальних спостережень деталізують відповідні процедури. Таким чином, ресурси MITRE ATT&CK дозволяють аналітикам CTI формувати деталізовані карти атаки (attack map) на основі технічних відомостей про TTPs.

Спеціалісти Агентства кібербезпеки та безпеки інфраструктури США (Cybersecurity and Infrastructure Security Agency, CISA) рекомендують використовувати картографування атак (attack mapping) для створення набору детальних карт можливих атак на інформаційну систему [9]. При цьому остаються невідомими способи формування відповідних шаблонів ознак події безпеки, що дозволять автоматизовано детектувати атаки за часом і простором інформаційної системи за допомогою комп'ютерних засобів IDS та SIEM.

Більшість інших відомих моделей APT атак також представлені у вигляді вербального опису етапів (тактик) атаки і їх смислового змісту [10] - [12]. Цінність таких моделей – вони допомагають виділити наступні загальні закономірності щодо різних APT атак:

– всі APT атаки спрямовані на конкретний ресурс інформаційної системи жертви (цільовий ресурс);

– незалежно від відмінності в цілях і засобах всі APTs проходять однакові етапи: зовнішня розвідка; проникнення в систему; доставка засобів впливу; внутрішня розвідка; створення та використання несанкціонованого каналу дистанційного управління; цільова акція атаки; приховування слідів атаки.

Недолік таких моделей – неможливість прямого застосування інфраструктурою кіберзахисту (IDS, SIEM) через відсутність загальної основи для алгоритмізації дій зловмисника в рамках етапів атаки.

В основі іншої групи моделей лежать різні математичні конструкції, що дозволяють уявити масштабні дії зловмисника у вигляді одного складного процесу. Одні такі моделі засновані на представленні у вигляді дерева атаки (графа), в якому елементи (гілки, листя) об'єднуються за допомогою логічних елементів AND або OR [13] - [15]. При використанні таких моделей на рівні оцінювання в SIEM може використовуватися мурашиний алгоритм оптимізації (Ant Colony Optimization, ACO). Такі моделі не вважаються найкращими, тому що вони складно зв'язуються з технологічними процесами в кіберсегменті [16]. Інша концептуальна модель, піраміда атаки, дозволяє відобразити траєкторію нападу в різних складових середовищах інформаційної системи [17]. Також виділяються моделі, які направлені на ідентифікацію атаки на ранніх етапах та прогнозують її розвиток за допомогою

прихованої марківської моделі (Hidden Markov Model, HMM) [18]. Практичне застування таких моделей обмежене наявністю ряду невизначеностей відносно прихованих станів і відповідної складністю реалізації алгоритму Вітербі (Viterby algorithm) для визначення значень станів марківського процесу (тобто, детектування атаки).

**Метою статті є** розробка моделей, що дозволяють аналітикам CTI деталізувати карти прогнозування APT атак до рівня автоматизованого детектування комп'ютерними засобами інфраструктури кіберзахисту.

**Основний матеріал досліджень.** За основу проведених досліджень було обрано інформаційний підхід до представлення комплексу наступних пов'язаних процесів:

– підготовки та реалізації кібератаки зловмисником;

– організації захисту від цього нападу за допомогою інфраструктури кіберзахисту:

– забезпечення розвідкою загроз інформацією, що необхідна для результативного функціонування інфраструктури кіберзахисту.

Інформаційний підхід заснований на такому розумінні сутності інформації, що дозволяє з однакових позицій представити вісь комплекс зазначених процесів. Для цього була обрана концепція атрибутивно-трансферної природи інформації (Attributive-Transfer Nature of Information, ATNI). Ця концепція дозволяє представити основні процеси, що складають сутність CTI, у вигляді сукупності різних інформацій та операцій з цією інформацією. На відміну від інших підходів до інформації ATNI дозволяє представити конкретну інформацію та її зміст (семантику) в явному вигляді як окремий фізичний об'єкт. В свою чергу, кожне перетворення інформації (інформаційний процес) може бути представлено фізичним процесом з особливими властивостями. Крім цього, ATNI дозволяє кожен інформаційний об'єкт описати за допомогою математичної мови теорії множин. Такий опис відкриває можливості для подолання невизначеності вербального опису та переходу до формалізованого опису процесів CTI та кіберзахисту за допомогою обчислювальних алгоритмів. Це сприяє розробці відповідних програмних засобів автоматизації. Розглянемо більш детально сутність цього підходу.

**1. Концепція атрибутивно-трансферної природи інформації.**

Особливістю концепції ATNI [19] є те, що вона не пояснює інформацію за допомогою поріднених термінів "відомості", "дані" "знаки", "знання", "ментальні представлення", "семантика", "інтелект", "свідомість" та багато інших, що самі часто пояснюються через "інформацію". ATNI розглядає її тільки як фізичний об'єкт, що сформований особливим чином за допомогою фізичного впливу. Термін "інформація" розкривається за допомогою наступного поняття (концепту):

*інформація* про об'єкт *A* в об'єкті *B*, $I(A,B)$ – це властивість об'єкта *B*, що придбана в результаті фізичної взаємодії з іншим об'єктом *A* і є відображенням властивості цього об'єкту *A*.

Три приклади, що пояснюють цей концепт. Проміні сонця сформували тінь скелі, що повторює форму скелі. Друга ситуація: на вологому ґрунті дика тварина залишає ланцюжок слідів, форма кожного з яких містить унікальні особливості, як виду, так і самої тварини. Третя ситуація: людина – свідок небезпечної події (сильний землетрус в океані, раптове виверження вулкана чи ін.) складає текстове повідомлення. Передане каналами зв'язку повідомлення може призвести до кардинальних змін у житті суспільства (запровадження надзвичайного стану, евакуація населення тощо). Загальне, що поєднує всі ці різні ситуації – наявність таких фізичних взаємодій між об'єктами, результатами яких є нові придбані властивості об'єктів, що відображають властивість об'єкту, що впливає.

Запропонований концепт може бути "більш суворим", якщо для його опису використати математичні конструкції теорії множин:

$$I(at_iA:B)=(B,at_{j+1}B \mid f_{map}{}^{(tI)}:at_iA\,I \rightarrow at_{j+1}B\,, \qquad (1)$$

тобто, інформація про властивість (атрибут) $at_iA$ об'єкту *A* в об'єкті *B* – це сам об'єкт *B* з придбаною (в момент часу $t_1$) властивістю $at_{J+1}B$, яка сформована впливом $f_{map}{}^{(t1)}$, що відображає властивість $at_iA$ ($at_iA$=*"полусфера"*) в нової властивості $at_{J+1}B$

($at_{J+1}B$=*"полусфера"*). У цьому описі кожний об'єкт представляє собою множину його властивостей (атрибутів):

$$A=\{at_iA\},\ i=\overline{1,I};\quad B=\{at_jB\},\ j=\overline{1,J}\ . \tag{2}$$

Кожна властивість об'єкту розглядається як впорядкована сукупність елементів цього об'єкту, що дає можливість представити її як підмножину на декартовому добутку множин, що є осями системи координат в місці розташування цього об'єкту. Приклад:

$$"напівсфера"=at_iA\subset X_A\times Y_A\times Z_A, \tag{3}$$

де $X_A$, $Y_A$, $Z_A$ – вісі системи координат, що дозволяють визначити місце розташування об'єкту *A*. Кожний елемент підмножини $at_iA$ – упорядкована трійка відповідних елементів вісей координат:

$$(x_A,y_A,z_A)\in at_iA="напівсфера". \tag{4}$$

Зрозуміло, що вираз (3) не обмежується застосуванням тільки для властивості *"напівсфера"*, яка використовувалась тільки для візуалізації прикладу.

Запропонована парадигма інформації дозволяє визначити наступні супутні поняття:

1) об'єкт *A* – це *джерело інформації* $I(at_iA:B)$;

2) об'єкт *B* – це *носій інформації* $I(at_iA:B)$, який визначає місцеположення інформації в просторі-часі;

3) властивість об'єкту *A* $at_iA=essence\left[I(at_iA:B)\right]$ – це *сутність інформації* $I(at_iA:B)$;

4) придбана властивість об'єкту *B* (носій інформації) $at_{j+1}B$ – це *семантика (сенс) інформації* $I(at_iA:B)$, тобто, $at_{j+1}B=semantic\left[I(at_iA:B)\right]$. В семантиці інформації відображена властивість об'єкту *A*, шо раніше була визначена як сутність конкретної інформації $I(at_iA:B)$*)*. Якщо розглядаються декілька семантик інформації одного носія *B*, то семантику інформації можливо означати просто як $semantic(A)$;

5) $f_{map}$ – оператор відображення (індекс *map* – від англійського слова *mapping*, відображення) визначає характер взаємодії об'єктів під час формування інформації.

Розглянута парадигма ATNI була побудована на твердженні, що інформація, як особливий феномен фізичного світу могла, існувати ще до появи життя (біологічних систем). Такий підхід дозволив описати інформацію через терміни, які можна пов'язати із неживою природою: об'єкт, властивість, вплив, відображення. Приклад інформації з часів до появи життя – тінь скелі, що сформована сонячним світлом та повторює форму скелі. Така інформація

$$I(at_iA:B)=I(форма\ скелі:поверхня)=тінь\ скелі$$

існувала тільки при наявності сонячного світла, яке виконувало роль інфоутворюючого впливу ($f_{map}$). На той час ця інформація ніде не використовувалася та зникала разом зі світлом. Але у подальшому цей феномен став масштабна використовуватися спочатку в біологічних, а потім, в технічних кібернетичних (керованих) системах для визначення їх поведінки в залежності від впливу зовнішнього середовища. Можливо також впевнено стверджувати, що інформація виконує основну роль в створенні та функціонуванні синергетичних (самоорганізованих) систем.

Для подальшого розгляду інформаційних процесів пропонується впровадити наступне поняття:

*Інформаційне середовище кібернетичної системи (далі – інформаційне середовище, Information Environment, IE) – це набір взаємопов'язаних елементів однакової фізичної природи (далі – операційні елементи, Operating Elements, OE), який дозволяє:*

– *фіксувати результати інформаційних впливів у вигляді зміни значень властивостей цих елементів (відповідно до парадигми ATNI набуті значення властивостей – це семантики інформації, далі – семантики);*

– *зберігати семантики інформації;*

– *формувати різні семантичні конструкції на основі семантик інформації;*

– *виконувати різні операції над семантиками та семантичними конструкціями (порівняння, об'єднання, аналіз, синтез та багато інших);*

– *створювати та забезпечувати процеси використання семантик на користь інших систем;*

– *на основі семантик формувати інформаційні впливи для обміну семантичними конструкціями з іншими кібернетичними системами.*

У людини та вищих тварин, яких відносять до біологічних кібернетичних систем, можливо виділити наступні два види найбільш відомих інформаційних середовищ:

– білкове інформаційне середовище (Protein Information Environment, PIE);

– нейронне інформаційне середовище (Neural Information Environment, NIE).

Роль операційних елементів PIE виконують білки, які у своїй структурі відображають та зберігають особливості ділянок ДНК біологічної істоти. У свою чергу, білки є основним будівельним матеріалом для формування та забезпечення функціонування біологічного організму. Основу NIE складають нейрони, в наборах (патернах) яких за допомогою органів почуття (сенсорів) відображаються інформаційні впливи ($f_{map}$) зовнішнього/внутрішнього середовища біологічного організму. На основі порівняння поточних семантик та набутого досвіду (тобто, раніше сформованих семантик) визначається траєкторія поведінки системи.

Технічні кібернетичні системи, що керуються за допомогою комп'ютерних засобів, використовують комп'ютерне інформаційне середовище (*Computer Information Environment, CIE*). Операційними елементами *CIE* є електронні регістри пам'яті, з'єднані лініями передачі електричних сигналів. Кожен регістр складається із сукупності тригерів. Один тригер – один осередок пам'яті. Тригери – це напівпровідникові пристрої, які під впливом електричного сигналу можуть перемикатися в один із двох можливих станів. Умовні назви значень станів – логічні двійкові одиниці "1" чи "0". За допомогою сенсорів кібернетичних систем (засобів вводу/виводу) формуються семантики *CIE* у вигляді наборів логічних двійкових одиниць (бітів), що зберігаються в регістрах, передаються дискретними електричними сигналами по лініям зв'язку, перетворюються за допомогою арифметично-логічних пристроїв (АЛП) обчислювальних процесорів. АЛП дозволяють на основі семантик від сенсорів формувати різні семантичні конструкції, які раніше не існували в цьому середовищі.

**2. Інфраструктура кіберзахисту та її процеси функціонування.**

За основу аналізу сутності кіберзахисту корпоративної інформаційної системі було обрано відомий підхід [20], [21], що представляє кіберзахист у вигляді безперервного процесу з постійно повторюваного циклу керування кібербезпекою. У загальному вигляді цей цикл представлений на рисунку 3.


Рисунок 3 – Цикл керування кібербезпекою

Всі заходи циклу поділяються на п’ять етапів. Заходи кіберзахисту кожного етапу повинні виконувати окрему функцію. Кожна функція має назву та загальний опис їх змісту:

1) «Ідентифікація ризиків кібербезпеки» (Identify, ID).

Формування розуміння складу інформаційної системи, умов її функціонування, переліку інформаційних ресурсів, що підтримують надання життєво важливих послуг та функцій. Визначення ризиків кібербезпеки, що пов'язані з цими послугами та функціями. Обґрунтований вибір пріоритетів захисту та конкретних заходів для впровадження;

2) «Кіберзахист» (Protect, PR).

Визначення (розробка) відповідних методів, засобів, процедур кіберзахисту. Впровадження в інформаційну систему прийнятих рішень за допомогою інфраструктури кіберзахисту;

3) «Виявлення кіберінцидентів» (Detect, DE);

Реалізація заходів своєчасного виявлення кіберінцидентів.

4) «Реагування на кіберінциденти» (Respond, RS)

Прийняття рішення щодо можливих заходів зниження негативного впливу визначеного кіберінциденту.

5) «Відновлення стану кібербезпеки» (Recover, RC).

Реалізація заходів зниження негативного впливу кіберінциденту та відновлення поточного стану кібербезпеки.

Для впровадження циклу заходів кіберзахисту потрібна інфраструктура кіберзахисту (ІК), яка впроваджується в середовище інформаційної системи. Основою такої ІК є сукупність апаратних та програмних комп’ютерних засобів, які відносяться до таких функціональних компонентів:

1) засоби системи виявлення вторгнень (Intrusion Detection System, IDS);
2) засоби системи запобігання вторгненням (Intrusion Prevention System, IPS);
3) засоби центру операцій кібербезпеки (the Cyber Security Operations Center, CSOC, або просто SOC);
4) засоби системи управління подіями та інформацією безпеки SIEM (Security Information and Event Management);
5) засоби та заходи розвідки кіберзагроз (Cyber Threat Intelligence, CTI).

Ці компоненти інфраструктури кібербезпеки поєднується з циклом заходив кіберзахисту відповідними процесами (табл. 1).

Таблиця 1 – Відповідність процесів інфраструктури кіберзахисту функціям циклу

| Функція циклу | Процеси інфраструктури кіберзахисту |
|---|---|
| 1. Ідентифікація ризиків (ID) | CTI на основі аналізу ресурсів та сервісів (послуг) інформаційної системи визначає перелік загроз. Для кожної загрози визначаються технічні ознаки (індикатори компрометації), які можуть поєднуватися в шаблони ознак подій безпеки (security event attributes pattern, SEAP). Визначаються апаратні та програмні засоби для інфраструктури кіберберзахисту, заходи їх використання. |
| 2. Кіберзахист (PR) | Всі засоби та заходи захисту впроваджується в середовище інформаційної системи. SOC – це організаційно-технічна система, компонентами якої є офіцери безпеки, засоби SIEM та CTI. Режими роботи засобів IDS конфігуруються на основі SEAP. Перевіряється роботоздатність всіх засобів. |
| 3. Виявлення кіберінцидентів (DE) | Засоби IDS порівнюють поточні елементарні події (трафіки, файли, обчислювальні процеси) в комп’ютерному середовищі з відомими шаблонами ознак подій безпеки (SEAP). У разі збігу шаблону з подією комп’ютерного середовища формується інформація безпеки (security information) про цю подію та передається для аналізу на засоби SIEM. За результатами аналізу |

Кінець таблиці 1

| | |
|---|---|
| | такої інформації офіцери безпеки (або автоматизовані процеси) приймають рішення про наявність інциденту кібербезпеки (кібератаки). |
| 4. Реагування на кіберінциденти (RS) | На основі досвіду та актуальних знань офіцери безпеки приймають рішення про відповідь на інцидент. За допомогою засобів SIEM формуються та направляються до засобів IPS відповідні команди. |
| 5. Відновлення стану кібербезпеки (RC) | Засобі IPS на основі отриманих команд реалізують прийнято рішення щодо відновлення стану кібербезпеки. |

**3. Структура моделі чотирьох інформаційних середовищ кібератаки.**

Проведені дослідження дозволили розробити модель чотирьох інформаційних середовищ кібератаки (model of four cyberattack information environments, далі – 4CAIE). Ця модель за допомогою інформаційного підходу на основі концепції ATNI дозволила поєднати та деталізувати:

- діамантову модель (Diamond Model, DM);
- модель ланцюжка кіберзнищення (Cyber Kill Chain, CKC);
- цикл керування кібербезпекою;
- інфраструктури кіберзахисту.

Структура моделі 4CAIE представлена на рисунку 4. Основою моделі є інформаційне середовище кібератаки (CyberAttack Information Environment, CAIE) , що складається з 4-х сегментів, в яких відображаються різні основні аспекти кібератаки та захисту від неї. Сегменти моделі сформовані наступними сутностями: противник (Adversary), жертва (Victim), ментальне інформаційне середовище (Mental Information Environment, MIE), комп'ютерне інформаційне середовище (Computer Information Environment, CIE), або його розповсюджена назва – кіберпростір (Cyberspace).

CAIE як множину можливо представити декартовим добутком двох кортежей:

$$\text{CAIE}=\left(\text{Advensory, Victim}\right)\times\left(\text{MIE, CIE}\right). \quad (5)$$

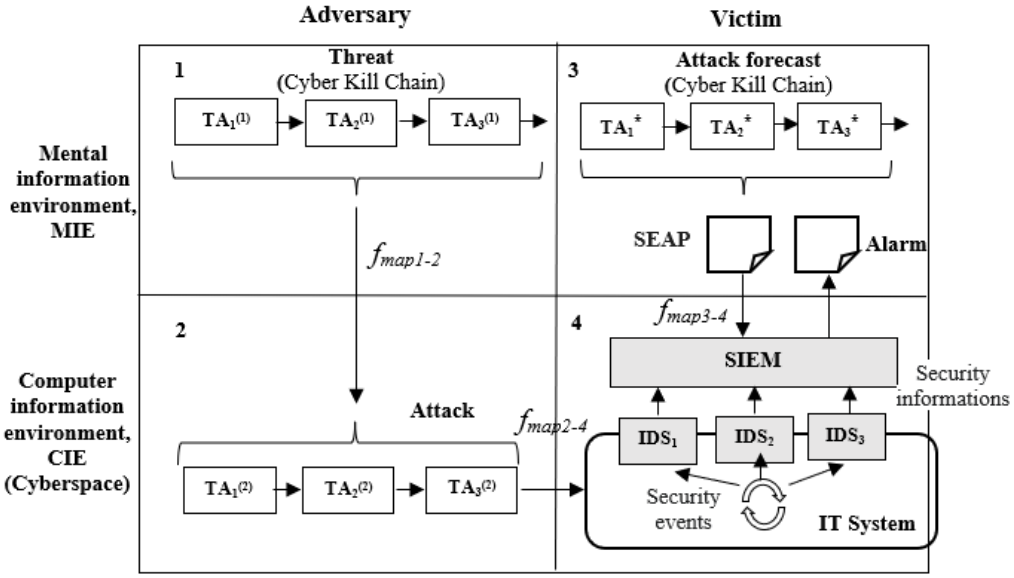


Рисунок 4 – Модель 4-х інформаційних середовищ кібератаки (4CIE)

У подальшому в рамках будемо розглядати наступні сегменти CAIE:

– сегмент 1 (MIE, Adversary) – це ментальне середовище противника, де визначається цільова жертва та формується план атаки на інформаційну систему жертви, (тобто, це сегмент загрози):

– сегмент 2 (CIE, Adversary) – це комп'ютерне середовище противника, засобами якого противник реалізує атаку на основі семантики раніше сформованої загрози (тобто, це сегмент атаки):

– сегмент 3 (MIE, Victim) – це ментальне середовище жертви, де формуються прогнози можливих кібератак (Attack Forecast) (далі, сегмент кіберзахисту);

– сегмент 4 (CIE, Victim) – це комп'ютерне середовище жертви, що реалізовано в відповідною інформаційною системою. В сегменті відображаються впливи атаки противника та дії жертви щодо кіберзахисту від цієї атаки (далі, сегмент кіберзахисту).

Сегменти 1-2 та 2-3 пов'язані між собою інформаційними впливами, які можливо представити наступними операторами:

$f_{map1-2}$ – оператор інформаційного впливу, що дозволяє перетворювати семантичні конструкції MIE в конструкції CIE. Реалізується людиною шляхом маніпулювання комп'ютерними засобами вводу-виводу даних (тобто, використовується людино-машинний інтерфейс);

$f_{map2-4}$ – оператор інформаційного впливу, що дозволяє перетворювати семантичні конструкції CIE сегменту 2 в семантичні конструкції CIE сегменту 4, шляхом передачі необхідних даних на відстань між сегментами за допомогою електромагнітних сигналів;

$f_{map3-4}$ – оператор інформаційного впливу, що дозволяє по аналогії з $f_{map1-2}$ перетворювати семантичні конструкції MIE жертви (прогнози атак) в конструкції CIE (шаблони індикаторів компрометації (SEAP) для засобів SIEM**).**

**4. Концепція моделі 4CIE.**

В рамках чотирьох інформаційних середовищ (сегментів) моделі можливо деталізувати та поєднати події, що розкривають сутність підготовки та реалізації APT, процеси захисту від неї та завдання розвідки кіберзагроз. Послідовно розглянемо події по сегментам.

1. Почнемо з сегменту 4. Його основу складає інформаційна система (ІС, або англомовною термінологією – система інформаційних технологій, IT-system). Для противника ця ІС виступає у ролі жертви. Комп'ютерні апаратні та програмні засоби ІС дозволяють реалізовувати різні технології обробки інформації (TOI) в інтересах персоналу ІС. Кожна TOI представляє собою динамічну за часом комбінацію, що складається з необхідної кількісті елементарних подій трьох видів відносно бітових наборів:

a) набори бітів, що зберігаються у комп'ютерному інформаційному середовищі – файли;

b) набори бітів, якими обмінюються комп'ютери – трафіки;

c) перетворення одних наборів бітів в інші за допомогою процесорів та відповідних програм комп'ютера – обчислювальні процеси (ОП).

2. Кожна елементарна подія в ІС може бути зареєстрована сенсором подій (комп'ютерний апаратний або апаратно-програмний засіб), який формує інформацію про цю подію (відповідний запис в журналі подій). Для відстеження подій, що впливають на стан кібербезпеки, використовуються сенсори безпеки, які прийнято називати засобами системи виявлення вторгнень (Intrusion Detection System, IDS). Вся інформація про події безпеки (інциденти кібербезпеки) від всіх IDS збирається для подальшого аналізу засобами системи керування інформацією та подіями безпеки SIEM. За результатами аналізу даних засобами SIEM приймається рішення про наявність вторгнення в ІС.

3. Ментальне інформаційне середовище сегменту 1 фізично розміщується в голові зловмисника. В ньому на основі інформації про вразливості ІС жертви та відомостей про засоби та методи нападу формується план (семантична конструкція) проведення APT атаки. На hbceyre 4 цей план представлений у вигляді ланцюжка кіберзнищення (Cyber Kill Chain, CKC) та позначається як Threat (загроза). CKC складається з послідовності тактик (етапів) $TA_i^{(j)}$ ($i$ – номер етапу, верхній індекс $j$ – номер сегменту). На рис. 4 – тільки три тактики TA). Тобто, загрозу можливо представити наступним чином

$$\text{Threat}=\left(\text{TA}_1^{(1)}, \text{TA}_2^{(1)},\ldots, \text{TA}_i^{(1)}\right). \quad (6)$$

Шляхом маніпуляцій в сегменті 2 зловмисник реалізує загрозу в у вигляді семантик його кіберсередовища. Для цього за допомогою відповідних комп'ютерних засобів він реалізує оператор інформаційного впливу $f_{map1\text{-}2}$. Тобто, семантики сегменту 1 перетворюються у семантики сегменту 2:

$$\text{Attack}=f_{map1-2}(\text{Threat}) =$$

$$=f_{map1-2}\left[\left(\text{TA}_1^{(1)}, \text{TA}_2^{(1)},\ldots, \text{TA}_i^{(1)}\right)\right]=\left(\text{TA}_1^{(2)}, \text{TA}_2^{(2)},\ldots, \text{TA}_i^{(2)}\right). \quad (7)$$

4. Результатом реалізації семантик $\left(\text{TA}_1^{(2)}, \text{TA}_2^{(2)},\ldots, \text{TA}_i^{(2)}\right)$ є інформаційний вплив $f_{map\,2-4}$ на середовище 4. Цей вплив реалізується передачею необхідних даних на відстань між сегментами за допомогою електромагнітних сигналів. Вплив може бути реалізований або в режимі *on-line* (трафік через Інтернет), або в режимі *off-line* (приклад, зараження вірусом Stuxnet через USB-flash накопичувач – атака на ядерні об'єкти Ірану, 2010 рік).

5. З метою захисту від можливих загроз в сегменті 3 формується прогноз атаки

$$\text{Attack forecast} = \left(\text{TA}_1^{(3)}, \text{TA}_2^{(3)},\ldots, \text{TA}_i^{(3)}\right). \quad (8)$$

Прогноз атаки, що формується в ментальному середовищі жертви (сегмент 3), не може бути використаний в комп'ютерному середовищі інформаційної системи жертви (сегмент 4) для детектування атаки засобами кіберзахисту (IDS), якщо він носить загальний (вербальний) характер. Якщо визначені привила, за допомогою яких можливо прогноз представити у вигляді сукупності ознак елементарних подій, то можливо сформувати шаблони подій (інцидентів) безпеки SEAP.

$$\text{SEAP}=f_{map3-4}(\text{Attack forecast}). \quad (9)$$

У випадку коли інформація про події в кіберсегменті (формується засобами IDS) буде співпадати з ознаками подій безпеки шаблону SEAP (знаходиться в SIEM), то буде формуватися сигнал попередження Alarm.

Представлена концепція моделі 4CAIE дозволяє конкретизувати завдання CTI:

1) за допомогою вербального опису скласти прогноз атаки у вигляді послідовності етапів моделі CKC з деталізацією тактик, технік та процедур (TTPs);

2) в рамках визначеної тактики представити можливі техніки та процедури у вигляді елементарних подій кіберсередовища (трафіки, файли, обчислювальні процеси);

3) для набору елементарних подій тактики визначити індикатори компрометації подій (як правило це будуть бітові сигнатури);

4) розробити правила, за якими можливо формувати шаблон подій безпеки SEAP для прогнозу Attack forecast;

5) сформувати методику використання SEAP в рамках конфігурації інфраструктури кіберзахисту;

6) перевірити роботоздатність методики;

7) передати SEAP та методику її використання підрозділам підтримки інфраструктури кіберзахисту.

**5. Приклад використання моделі.**

За допомогою:

– кібернетичної моделі APT-атаки [22], що дозволяє представити дії зловмисника (суб'єкт керування) відносно системи-жертви (об'єкт керування) у вигляді послідовності повторюваних цифрових елементарних подій в кіберсегменті (цикл керування);

– запропонованої моделі 4CAIE, що уточнює завдання CTI відносно забезпечення інфраструктури кіберзахисту;

було розроблено спосіб визначення каналу керування APT-атакою [23]. Таки несанкціоновані канали є основою більшості APT-атак. Вони формуються, як правило, на етапі Installation моделі Cyber Kill Chain та експлуатуються зловмисником на етапі Command and Control (C2). Визначення наявності такого каналу ще до початку етапу цільової акції (Actions on Objectives) надає можливість припинити атаку. Такий підхід відповідає проактивної стратегії кіберзахисту.

Розроблений спосіб складається з наступних основних етапів:

1) формування структури багатоіндикаторного шаблону SEAP на основі конкретних характеристик корпоративної інформаційної системи;
2) визначення індикаторів каналу керування;
3) налаштування мережевих і хостових IDS відповідно до структури шаблону та визначених індикаторів;
4) збір інформації про події безпеки за простором та часом ІТ-системи;
5) аналіз інформації шаблону та формування гіпотези про наявність каналу керування;
6) подальший збір та аналіз інформації в рамках підтвердження гіпотези;
7) в разі підтвердження гіпотези – відслідковування подальшої поведінки зловмисника.

Шаблон SEAP для визначення каналу керування був розроблений у вигляді таблиці послідовності циклів, комірки якої містять індикатори подій двостороннього обміну даними (двійкові сигнатури). Така структура шаблону дозволяє визначати наявність каналу керування за результатами збору інформації про трафіки від хостових IDS та IDS на основі файрволу периметру системи-жертви. За результатами порівняння індикаторів шаблону з поточною інформацією про трафіки формуються мітки, які заповнюють комірки відповідних циклів. За результатами аналізу комірок послідовності циклів попередньо формуються гіпотези. Подальший аналіз гіпотез на основі міток наступних циклів підтверджує або ні наявність каналу керування атакою.

**Висновки.** В умовах широкомасштабного застосування складних кібератак актуальним стає завдання розробки таких карт прогнозування APT-атак, що дозволяють формувати шаблони ознак подій безпеки (security event attributes pattern, SEAP) для автоматизованого детектування комп'ютерними засобами інфраструктури кіберзахисту. В рамках проведених досліджень за допомогою:

– інформаційного підходу до опису процесів кібернападу та кіберзахисту (на основі концепії атрибутивно-трансферної природи інформації ATNI);

– діамантової моделі (Diamond Model), що поєднує візуально на загальному рівні поєднує основні аспекти кіберзагроз;

– моделі ланцюжка кіберзнищення (Cyber Kill Chain), що вербально на загальному рівні описує послідовність дій зловмисника в рамках складної атаки;

– було розроблено модель чотирьох інформаційних середовищ кібератаки (model of four cyberattack information environments, 4CAIE).

Модель візуально деталізує та поєднує події, що розкривають сутність підготовки та реалізації APT-атаки, процеси захисту від неї та завдання розвідки кіберзагроз щодо забезпечення конкретними даними комп'ютерних засобів ефективної інфраструктури кіберзахисту. Рівень деталізації моделі дозволяє застосовувати відомі математичні конструкції для опису подій та інформації безпеки. Такий підхід спрощує процедуру формування алгоритмів для засобів автоматизації процесів кіберзахисту.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] G. Johansen, *Digital Forensics and Incident Response. An intelligent way to respond to attacks*. Birmingham, UK: Packt Publishing Ltd, 2017.

[2] W. Tounsi, "What is Cyber Threat Intelligence and How is it Evolving?" in *Cyber-Vigilance and Digital Trust: Cyber Security in the Era of Cloud Computing and IoT*, W. Tounsi, Ed, Wilty, April 2019. [Online]. Available: https://media.wiley.com/product_data/excerpt/81/17863044/1786304481-46.pdf. Accessed on: June 19, 2023. doi: https://doi.org/10.1002/9781119618393.

[3] What is threat intelligence? IBM. 2023. [Online]. Available: https://www.ibm.com/topics/threat-intelligence. Accessed on: June 01, 2023.

[4] NIST Special Publication 800-150, Guide to Cyber Threat Information Sharing, 2016. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf. Accessed on: June 21, 2023.

[5] What is Threat Intelligence? VMware by Broadcom. 2023. [Online]. Available: https://www.vmware.com/topics/glossary/content/threat-intelligence.html. Accessed on: June 20, 2023.

[6] Diamond Model of Intrusion Analysis: A Quick Guide. Security Boulevard, 2023. [Online]. Available: https://securityboulevard.com/2023/03/diamond-model-of-intrusion-analysis-a-quick-guide. Accessed on: June 14, 2023.

[7] E. M. Hutchins, M. J. Clopperty, and R. M. Amin. "Intelligence-Driven Computer Network Defense. Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains", *Lockheed Martin Corporation*, 2009. [Online]. Available: https://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf. Accessed on: June 14, 2023.

[8] B. E. Strom, A. Applebaum, D. P. Miller, K. C. Nickels, A. G. Pennington, and C. B. Thomas, *MITRE ATT&CK: Design and Philosophy*, McLean, VA, USA: The MITRE Corporation. 2020. [Online]. Available: https://www.mitre.org/news-insights/publication/mitre-attck-design-and-philosophy. Accessed on: June 14, 2023.

[9] Best Practices for MITRE ATT&CK. Mapping, *Cybersecurity and Infrastructure Security Agency (CISA)*, 2023. [Online]. Available: https://www.cisa.gov/sites/default/files/2023-01/Best%20 Practices%20for% 20MITRE%20ATTCK%20Mapping.pdf. Accessed on: June 27, 2023.

[10] P. Chen, L. Desmet, and C. Huygens, "A study on Advanced Persistent Threats", in *Proc. 15th IFIP TC 6/TC 11 International on Conference Communications and Multimedia Security*, Aveiro, Portugal, 2014, pp. 63-72. doi: https://doi.org/10.1007/978-3-662-44885-4_5.

[11] *Mandiant M-Trends: The Advanced Persistent Threat*, Mandiant, 2010. [Online]. Available: https://wikileaks.org/hbgary-emails//fileid/27714/8307. Accessed on: July 07, 2023.

[12] D. E. Whitehead, K. Owens, D. Gammel, and J. Smith, "Ukraine Cyber-Induced Power Outage: Analysis and Practical Mitigation Strategies", in *Proc 2017 70th Annual Conference for Protective Relay Engineers (CPRE)*, College Station, TX, USA, 2017, pp. 1-8. doi: https://doi.org/10.1109/CPRE.2017.8090056

[13] S. A. Camtepe, and B. Yener, "Modeling and detection of complex attacks", in Proc. 2007 Third International Conference on Security and Privacy in Communications Networks and the Workshops – SecureComm 2007, Nice, France, 2007. pp. 234-243. doi: https://doi.org/10.1109/SECCOM.2007.4550338.

[14] F. Arnold, H. Hermanns, R. Pulungan, and M. Stoelinga, "Time-dependent analysis of attacks", in *Proc. International Conference on Principles of Security and Trust (POST-2014)*, Grenoble, France, pp. 285-305. doi: http://dx.doi.org/10.1007/978-3-642-54792-8_16.

[15] O. Flaten, and M. S. Lund, "How good are attack trees for modelling advanced cyber threats?", Norwegian Information Security Conference (NISK) 7(1), 2014.

[16] J. Navarro et al., "HuMa: A multi-layer framework for threat analysis in a heterogeneous log environment", in *Proc. 10th International Symposium Foundations and Practice of Security (FPS 2017)*, Nancy, France, 2017 Université de Strasbourg, France, ECAM Strasbourg-Europe, Schiltigheim, France, 2015, pp.144-159. [Online]. Available: http://fps2017.loria.fr/wp-content/uploads/2017/10/08.pdf. Accessed on: June 27, 2023.

[17] P. Giura, and W. Wang, "Using large scale distributed computing to unveil advanced persistent threats", *Science J*, vol. 1, iss. 3, pp.93-105, 2013. [Online]. Available: https://www.semanticscholar.org/paper/Using-Large-Scale-Distributed-Computing-to-Unveil-Giura-Wang/75e702d56a4a90f9c773a0e1fd0074cbe6910ead. Accessed on: June 27, 2023.

[18] Z. Cui, I. erwono, and P. Kearney, "Multi-stage attack modeling", in *Proc. Cyberpatterns 2013: The Second International Workshop on Cyber Patterns: Unifying Design Patterns with Security, Attack and Forensic Patterns*, pp. 78-89, 2013.

[19] I. Yakoviv, "Information, signs, knowledge and intelligence", *Information Technology and Security*, vol. 8, iss. 2, pp. 1-12, 2020. doi: http://dx.doi.org/10.20535/2411-1031.2020.8.2.222605.

[20] Адміністрація Держспецзв'язку (2021, Жовт. 06). Наказ № 601 Про затвердження Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної

інформаційної інфраструктури. [Електронний ресурс]. Доступно: https://cip.gov.ua/ua/news/nakaz-ad-2021-10-06-601.

[21] "Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1", *National Institute of Standards and Technology (NIST)*, 2018. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[22] І. Б. Яковів, "Кібернетична модель APT атаки", *Information Technology and Security*, vol. 6, iss. 1 (10), pp. 46-58, 2018. doi: http://dx.doi.org/10.20535/2411-1031.2018.6.1.153140.

[23] І. Яковів, А. Трохименко, та К. Глум, "Спосіб визначення каналу керування APT-атакою", *Information Technology and Security*, vol. 10, iss. 2 (17), pp. 176-188, 2021. doi: http://dx.doi.org/10.20535/2411-1031.2021.9.2.249899.

Стаття надійшла до редакції 06.09.2023.

## REFERENCE

[1] G. Johansen, *Digital Forensics and Incident Response. An intelligent way to respond to attacks*. Birmingham, UK: Packt Publishing Ltd, 2017.

[2] W. Tounsi, "What is Cyber Threat Intelligence and How is it Evolving?" in *Cyber-Vigilance and Digital Trust: Cyber Security in the Era of Cloud Computing and IoT*, W. Tounsi, Ed, Wilty, April 2019. [Online]. Available: https://media.wiley.com/product_data/excerpt/81/17863044/1786304481-46.pdf. Accessed on: June 19, 2023. doi: https://doi.org/10.1002/9781119618393.

[3] What is threat intelligence? IBM. 2023. [Online]. Available: https://www.ibm.com/topics/threat-intelligence. Accessed on: June 01, 2023.

[4] NIST Special Publication 800-150, Guide to Cyber Threat Information Sharing, 2016. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf. Accessed on: June 21, 2023.

[5] What is Threat Intelligence? VMware by Broadcom. 2023. [Online]. Available: https://www.vmware.com/topics/glossary/content/threat-intelligence.html. Accessed on: June 20, 2023.

[6] Diamond Model of Intrusion Analysis: A Quick Guide. Security Boulevard, 2023. [Online]. Available: https://securityboulevard.com/2023/03/diamond-model-of-intrusion-analysis-a-quick-guide. Accessed on: June 14, 2023.

[7] E. M. Hutchins, M. J. Clopperty, and R. M. Amin. "Intelligence-Driven Computer Network Defense. Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains", *Lockheed Martin Corporation*, 2009. [Online]. Available: https://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf. Accessed on: June 14, 2023.

[8] B. E. Strom, A. Applebaum, D. P. Miller, K. C. Nickels, A. G. Pennington, and C. B. Thomas, *MITRE ATT&CK: Design and Philosophy*, McLean, VA, USA: The MITRE Corporation. 2020. [Online]. Available: https://www.mitre.org/news-insights/publication/mitre-attck-design-and-philosophy. Accessed on: June 14, 2023.

[9] Best Practices for MITRE ATT&CK. Mapping, *Cybersecurity and Infrastructure Security Agency (CISA)*, 2023. [Online]. Available: https://www.cisa.gov/sites/default/files/2023-01/Best%20 Practices%20for% 20MITRE%20ATTCK%20Mapping.pdf. Accessed on: June 27, 2023.

[10] P. Chen, L. Desmet, and C. Huygens, "A study on Advanced Persistent Threats", in *Proc. 15th IFIP TC 6/TC 11 International on Conference Communications and Multimedia Security*, Aveiro, Portugal, 2014, pp. 63-72. doi: https://doi.org/10.1007/978-3-662-44885-4_5.

[11] *Mandiant M-Trends: The Advanced Persistent Threat*, Mandiant, 2010. [Online]. Available: https://wikileaks.org/hbgary-emails//fileid/27714/8307. Accessed on: July 07, 2023.

[12] D. E. Whitehead, K. Owens, D. Gammel, and J. Smith, "Ukraine Cyber-Induced Power Outage: Analysis and Practical Mitigation Strategies", in *Proc 2017 70th Annual Conference*

*for Protective Relay Engineers (CPRE)*, College Station, TX, USA, 2017, pp. 1-8. doi: https://doi.org/10.1109/CPRE.2017.8090056

[13] S. A. Camtepe, and B. Yener, "Modeling and detection of complex attacks", in Proc. 2007 Third International Conference on Security and Privacy in Communications Networks and the Workshops – SecureComm 2007, Nice, France, 2007. pp. 234-243. doi: https://doi.org/ 10.1109/SECCOM.2007.4550338.

[14] F. Arnold, H. Hermanns, R. Pulungan, and M. Stoelinga, "Time-dependent analysis of attacks", in *Proc. International Conference on Principles of Security and Trust (POST-2014)*, Grenoble, France, pp. 285-305. doi: http://dx.doi.org/10.1007/978-3-642-54792-8_16.

[15] O. Flaten, and M. S. Lund, "How good are attack trees for modelling advanced cyber threats?", Norwegian Information Security Conference (NISK) 7(1), 2014.

[16] J. Navarro et al., "HuMa: A multi-layer framework for threat analysis in a heterogeneous log environment", in *Proc. 10th International Symposium Foundations and Practice of Security (FPS 2017)*, Nancy, France, 2017 Université de Strasbourg, France, ECAM Strasbourg-Europe, Schiltigheim, France, 2015, pp.144-159. [Online]. Available: http://fps2017.loria.fr/wp-content/uploads/2017/10/08.pdf. Accessed on: June 27, 2023.

[17] P. Giura, and W. Wang, "Using large scale distributed computing to unveil advanced persistent threats", *Science J*, vol. 1, iss. 3, pp.93-105, 2013. [Online]. Available: https://www.semanticscholar.org/paper/Using-Large-Scale-Distributed-Computing-to-Unveil-Giura-Wang/75e702d56a4a90f9c773a0e1fd0074cbe6910ead. Accessed on: June 27, 2023.

[18] Z. Cui, I. erwono, and P. Kearney, "Multi-stage attack modeling", in *Proc. Cyberpatterns 2013: The Second International Workshop on Cyber Patterns: Unifying Design Patterns with Security, Attack and Forensic Patterns*, pp. 78-89, 2013.

[19] I. Yakoviv, "Information, signs, knowledge and intelligence", *Information Technology and Security*, vol. 8, iss. 2, pp. 1-12, 2020. doi: http://dx.doi.org/10.20535/2411-1031.2020.8.2.222605.

[20] Administration of the State Service for Special Communications (2021, Oct. 06). Order No. 601, On Approval of Methodological Recommendations on Increasing the Level of Cyber Protection of Critical Information Infrastructure. [Online]. Available: https://cip.gov.ua/ua/news/nakaz-ad-2021-10-06-601.

[21] "Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1", *National Institute of Standards and Technology (NIST)*, 2018. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[22] I. Yakoviv, "APT cyber attack model", *Information Technology and Security*, vol. 6, iss. 1 (10), pp. 46-58, 2018. doi: http://dx.doi.org/10.20535/2411-1031.2018.6.1.153140.

[23] I. Yakoviv, A. Trokhymenko, та K. Hlum, "A method of determining the control channel of an APT attack", *Information Technology and Security*, vol. 10, iss. 2 (17), pp. 176-188, 2021. doi: http://dx.doi.org/10.20535/2411-1031.2021.9.2.249899.

IHOR YAKOVIV

## MODEL OF FOUR CYBER ATTACK INFORMATION ENVIRONMENTS

The basis of the functioning of the modern cyber defense infrastructure of the corporate IT system is the procedure of comparing current events in the computer environment with the security event indicator. If the indicator matches the corresponding event, security information about this event is generated and transmitted to the SIEM for analysis. Based on the results of the analysis, a decision is made about the existence of a cyber security incident. At the next stage, a decision is made and implemented, which restores the state of cyber security. A mandatory condition for the effective cyber defense infrastructure is the availability of knowledge about possible cyber threats and relevant signs (indicators) of security events at the technical level of computer systems.

Cyber threat intelligence (CTI) is responsible for forming signs of security events. In the conditions of large-scale application of common repetitive cyberattacks, the main function of CTI was to identify simple technical features called indicators of compromise (IOCs). Bit sequences (signatures) are used as such IOCs.

In the conditions of large-scale application of complex cyberattacks, the task of developing such APT attack forecasting maps that allow the formation of security event attributes pattern (SEAP) for automated detection by computer means of cyber defense infrastructure becomes urgent.

The article is devoted to the development of a model that, with the help of an attribute-transfer approach to the essence of information, allows to formalize the processes of cyber protection. The model visually details and combines the events that reveal the essence of the APT attack preparation and implementation, the processes of protection and the task of cyber threat intelligence to determine specific data for the means of an effective cyber defense infrastructure. The level of detail of the model allows the application of known mathematical constructions to describe security events and security information. This approach simplifies the forming algorithms for automating cyber protection processes.

**Keywords:** nature of information, mental information environment, computer information environment, cyber defense infrastructure, proactive defense strategy, cyber threat intelligence, SIEM, IDS/IPS, APT prediction, indicators of compromise, security event pattern, cyber security management cycle.

**Яковів Ігор Богданович**, кандидат технічних наук, доцент, доцент кафедри кібербезпеки і застосування автоматизованих інформаційних систем і технологій, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна, ORCID 0000-0001-7432-898X, iyakov52@gmail.com.

**Yakoviv Ihor**, candidate of technical sciences, associate professor, associate professor at the cybersecurity and application of information systems and technology academic department, Institute of special communication and information protection of National technical university of Ukraine "Igor Sikorsky Kyiv polytechnic institute", Kyiv, Ukraine.