DOI 10.20535/2411-1031.2025.13.2.344710
УДК 004.056.53:621.391

ІГОР ЯКОВІВ,
ДМІТРО ШАРАДКІН,
ВАСИЛЬ КУЛІКОВ

# МОДЕЛІ ІНТЕГРАЦІЇ ІНФОРМАЦІЇ РОЗВІДКИ КІБЕРЗАГРОЗ

В умовах постійного зростання обсягів інформації про атаки на інформаційні системи актуальним є завдання підвищення результативності процесів розвідки кіберзагроз. Як правило, всю інформацію, що супроводжує ці процеси називають інформацією розвідки кіберзагроз, не поділяючі її за сутністю конкретного процесу. З іншого боку, опис структури комплексу всіх процесів має дуже загальний характер. Це все веде до високого рівня невизначеностей у опису розвідки кіберзагроз, що значно затрудняє впровадження класичних технологій автоматизації, оцінювання їх необхідності та ефективності. Відсутність конкретики в розумінні інформаційних процесів також заважає впровадженню засобів штучного інтелекту: складно визначити місце застосування та принципову можливість навчання нейронної мережі на даних розвідки кіберзагроз.

Одним з напрямків подолання цієї проблеми може бути використання формалізованих конструкцій, що описують зв'язок між основними складовими процесу формування та застосування розвідувального продукту. В рамках досліджень на основі парадигми атрибутивно-трансферної природи інформація, засобів системного та семантичного аналізу були розроблені метод структурного аналізу інформаційних процесів та метод семантичного синтезу базових понять. Використання цих методів дозволило сформувати:

- базовий набір узгоджених понять розвідки кіберзагроз;
- модель ролі (функції) розвідки загроз в процесі кіберзахисту;
- модель процесів розвідки кіберзагроз.

Результати досліджень дозволяють представити розвідку кіберзагро у вигляді сукупності (інформаційно-функціональної структури) узгоджених інформаційних процесів. Для кожного з цих процесів визначена семантика інформації та сутність її перетворень. З метою уточнення до потрібного рівня конкретизації кожний з процесів також може бути представлений інформаційно-функціональної структурою. Запропоновані моделі дозволяють класифікувати інформацію розвідки загроз та формувати структури для її інтеграції в рамках запровадження класичних автоматизованих технологій обробки. Значно спрощується процедура аналізу можливості застосування технологій штучного інтелекту.

За результатами досліджень розроблена комп'ютерна система для підтримки процесів керування ризиками кіберзагроз корпоративної інформаційної системи.

**Ключові слова:** розвідка кіберзагроз, інфраструктура кіберзахисту, інформаційно-функціональна структура, природа інформації, інформаційні процеси, інтеграція інформації, розвідувальний продукт, синтез понять, штучний інтелект, автоматизація.

**Постановка проблеми.** Зростання обсягів інформації про кіберзагрози та ускладнення її семантики супроводжується необхідністю удосконалення відповідних інформаційних технологій збору, інтеграції, зберігання та аналізу. Основою розробки таких технологій є структури, що формалізовано описують перелік об'єктів, які відображаються в інформації розвідки, їх сутність та взаємозв'язок. Великий обсяг інформації про розвідку кіберзагроз, як правило, носить дуже загальний характер та супроводжується високим рівнем семантичної та структурної невизначеності. Це не дозволяє деталізовано представити розвідку кіберзагроз комплексом узгоджених процесів, що значно звужує можливості їх алгоритмізації та впровадження ефективних інформаційних технологій.

Вирішення проблеми між невизначеністю процесів розвідки кіберзагроз та необхідністю підвищення їх ефективності на основі застосування інформаційних технологій є актуальним завданням.

**Аналіз останніх досліджень і публікацій.** *Розвідка кіберзагроз* (cyber threat intelligence, CTI), або *розвідка загроз* (threat intelligence, TI ), пов'язують з інформацією, даними або знаннями про різни аспекти діяльності у сфері кіберзахисту [1]-[4]. Типовим поняттям, що розкриває сутність CTI, може бути наступне [5]:

*Розвідка кіберзагроз – це інформація про кіберзагрози, яка була зібрана, перетворена, проаналізована, інтерпретована або збагачена для забезпечення необхідного контексту для процесів прийняття рішень.*

Таке визначення та багато інших подібних мають загальний, неконкретний характер опису сутності *інформації про кіберзагрози,* технологій її формування та використання. Це значно впливає на вирішення проблем щодо удосконалення результативності CTI, підвищення її ефективності. В свою чергу, відзначається залежність ефективності CTI від подолання постійно існуючих проблем, таких як [6]:

– динамічний характер кіберзагроз, що вимагає постійної адаптації стратегій виявлення загроз до постійно масштабуємого ландшафту кібератак;

– великий обсяг даних, що ускладнює розмежування реальних ризиків загроз та хибнопозитивних результатів.

Серед актуальних напрямів досліджень в напрямку підвищення ефективності найбільш часто виділяють наступні [6]:

1) Інтеграція розвідки кіберзагроз в інфраструктуру безпеки організації для проактивної обробки та результативного використання даних CTI;

2) Впровадження методів поведінкового аналізу у виявленні загроз на основі штучного інтелекту;

3) Розробка платформ CTI, що покращують оперативність організації та підтримують виявлення загроз, забезпечуючи обмін інформацією про загрози в режимі реального часу.

В рамках інтеграції інформації CTI в інфраструктуру кібербезпеки організації пропонується використання платформ, що агрегують інформацію розвідки загроз від відкритих джерел (OSCTI) за допомогою методів штучного інтелекту (ШІ). Об'єднання структурованих та неструктурованих даних з різних джерел може бути здійснено за допомогою методики машинного навчання *BERT* (англ. *Bidirectional Encoder Representations from Transformers*, двоспрямовані кодувальні представлення з трансформерів) для підвищення точності ідентифікації об'єктів, використовуючи механізм уваги, та модифікованій алгоритм Левенштейна для ефективного об'єднання даних [7], [6]. Сформований граф знань з кібербезпеки (cybersecurity knowledge graph, CKG) застосовується для виявлення передових постійних загроз (APT) та атак нульового дня [10]. Недоліком платформи є залежність її продуктивності від постійної зміни ландшафту кіберзагроз [6]. Запропонована структура (CKG) зв'язує між собою тільки інформацію про кіберзагрози з відкритих джерел залежить від необхідності регулярного донавчання нейронної мережі та не залежить від інформації про інфраструктуру кіберзахисту.

Платформа підтримки розвідки кіберзагроз THREATRAPTOR також побудована на концептах інтеграції інформації про кіберзагрози з відкритих джерел та поведінкового аналізу у виявленні загроз на основі штучного інтелекту [8]. Інтеграція забезпечується на основі обробки природної мови (NLP) повідомлень OSCTI зі спеціальною мовою запитів пошуку (TBQL) цих повідомлень. Таке поєднання технологій дозволяє виявляти тонкі моделі можливої поведінки зловмисника, які часто залишаються непоміченими під час традиційних аудитів стану кібербезпеки [6], [8]. Відмінністю цієї платформи від попередньої є її можливість працювати з неструктурованої інформацією OSCTI, тобто працювати без наявності графів знань з кібербезпеки. З одного боку, це дозволяє швидше реагувати на зміни ландшафту кіберзагроз, а з іншого – повністю не долає проблему вчасного донавчання

нейронної мережі. Питання інтеграції інформації OSCTI з інфраструктурою кібербезпеки залишаються відкритими.

Платформа CTI FedCT для інфраструктури кіберзахисту Інтернет речей (IoT) пропонує застосовувати розподілений ШІ для виявлення кіберзагроз на основі аномальної поведінки в системі віддаленого моніторингу пацієнтів (Remote Patient Monitoring systems, RPM) [11]. Подолання проблеми адаптації агентів ШІ до масштабування ландшафту кіберзагроз пропонується на основі застосування децентралізованого навчання на основі неінтегрованих даних про всіх пацієнтів системи. Аналіз наданої структури та процесів CTI для RPM системи дозволяє стверджувати про наявність підміни понять під час розробки цієї платформи. Під терміном *кіберзагроза* було застосовано поняття *загроза здоров'ю пацієнта*. Така заміна привела до того, що замість платформи CTI була створена платформа виявлення стану погіршення здоров'я пацієнта на основі аномалій в параметрах стану організму. Таке погіршення ніяким чином не залежить від зловмисного втручання в кіберсистему. Ймовірно до такої ситуації привела семантична невизначеність в поняттях *кібербезпека, кберзагроза, розвідка кіберзагроз, інфрвструктура кіберзахисту*.

За результатами проведеного аналізу можливо стверджувати що застосування ШІ є актуальною тенденцією розвитку платформ CTI в напрямку підвищення ефективності обробки постійно зростаючих обсягів інформації про кіберзагрози. Основними стримуючими факторами цього розвитку є:

– ландшафт загроз, що постійно розширюються. Це формує проблему постійної актуалізації даних навчання нейронних мереж платформ ШІ;

– невизначеність в структурах інтеграції:

a) інформації про загрози з різних джерел між собою;

b) інформації розвідки кіберзагроз з інформацією інфраструктури кіберзахисту.

Це впливає на коректне визначення сутності завдання ШІ, що вирішується в рамках системи розвідки кіберзагроз.

В умовах зростання обсягів зловмисних дій в кіберпросторі актуальним е завдання розробки формалізованих моделей інтеграції інформацій розвідки кіберзагроз та інфраструктури кіберзахисту для розробки ефективних платформ керування кібербезпекою.

**Метою роботи** є розробка формалізованих моделей класифікації, інтеграції та обробки інформації про загрози для впровадження ефективних технологій керування кібербезпекою інформаційних систем.

**Основний матеріал досліджень.** Для формування формалізованих моделей в рамках досліджень було розроблено методи *структурного аналізу інформаційних середовищ* (САІС) CTI та *семантичного аналізу базових понять* (САБП) у сфері кібербезпеки. Розглянемо сутність цих методів.

**1. Метод структурного аналізу інформаційних процесів.** Метод САІП є спеціалізованою версією методу ієрархічної декомпозиції. Основою методу є застосування парадигми *атрибутивно-трансферної природи інформації* (Attributive-Transfer Nature of Information, ATNI). ATNI [12] розглядає інформацію 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 $A$.

Для застосування парадигми в рамка математичної формалізації опису інформаційних процесів поняття "інформація" може бути представлено більш точно:

$$I\left(\alpha t_i A : B\right) = \left(B, \alpha t_{j+1} B\right) \middle| f_{map}^{(t_1)} : \alpha t_i A \mapsto \alpha t_{j+1} B, \quad (1)$$

тобто, інформація про властивість (атрибут) $\alpha t_i A$ об'єкту $A$ в об'єкті $B$ – це сам об'єкт $B$ з придбаною (в момент часу $t_1$) властивістю $\alpha t_{j+1} B$, яка сформована впливом $f_{map}^{(t_1))}$, що

відображає властивість $\alpha t_i A$ (наприклад, $\alpha t_i A =$ "напівсфера") у новій властивості $\alpha t_{j+1} B$ ( $\alpha t_{j+1} B =$ "напівсфера"). У цьому описі кожний об'єкт представляє собою множину його властивостей (атрибутів):

$$A = \{\alpha t_i A\}, i = 1,\ldots, I; \quad B = \{\alpha t_j B\}, j = 1,\ldots, J. \tag{2}$$

У свою чергу, властивість об'єкту можливо розглядати як впорядковану сукупність елементів цього об'єкту. Тобто представляти її як підмножину на декартовому добутку множин, що є осями якийсь системи координат. Наприклад, якщо місце розташування цього об'єкту пов'язано із просторовими осями координат $X_A, Y_A, Z_A$, то така властивість як конкретна фізична форма може бути описана формулою (3):

$$\text{"напівсфера"} = \alpha t_i A \subset X_A \times Y_A \times Z_A. \tag{3}$$

На відміну від інших підходів ця парадигма дозволяє представити конкретну інформацію та її зміст (семантику) в явному вигляді як окремий фізичний об'єкт з конкретним місцем розташування в комп'ютерній системі. Наприклад, якщо $B$ – це файл, в якому є придбана властивість $\alpha t_{j+1} B$, то семантику інформації $I(\alpha t_i A : B)$ можливо представити формулою (4):

$$\alpha t_{j+1} B = semantic\left[I(\alpha t_i A : B)\right]. \tag{4}$$

В рамках інформаційної системи такими фізичними об'єктами є трафіки та файли, які пов'язані мж собою обчислювальними процесами (перетвореннями $f_{map}$). Всі ці складові (трафіки, файли, обчислювальними процеси) можуть бути ідентифіковані та зареєстровані комп'ютерними засобами.

Парадигма ATNI дозволяє любу технологію обробки інформації (*information processing technology, IPT*) представити набором інформаційних процесів (*information process*, *IP*):

$$IPT = \{IP_1, IP_2, \ldots, IP_n, \ldots, IP_N\}, \tag{5}$$

де $N$ – кількість процесів.

В свою чергу, кожний *IP* може бути представлений "впорядкованою трійкою":

$$IP_n = \left\{I_{in}^{(n)}, F_m^{(n)}, I_{out}^{(n)}\right\}, \tag{6}$$

де: $I_{in}^{(n)}, I_{out}^{(n)}$ – вхідна та вихідна інформації процесу $n$;

$F_m^{(n)}$ – оператор перетворення (*функція,* не завжди тотожно поняттю *математична функція*).

В рамках структурного аналізу кожну *IPT* можливо представити системою з *інформаційно-функціональною структурою (ІФС)*, що відображає всі складові інформаційних процесів та зв'язок між ними. В цьому випаду структурними компонентами ІФС будуть інформаційні перетворення $F^{(n)}$ всіх процесів *IPT*, а взаємозв'язок між компонентами буде відображати інформацію цих процесів (вихідна інформація одного процесу $IP_n$ буде вхідною інформацією наступного процесу $IP_{n=1}$). На рисунку 1 надається приклад ІФС системи, що складається з чотирьох інформаційних процесів.

Використання ІФС в рамках структурного аналізу дозволяє отримати формалізований опис (графічний та математичний) складного інформаційного середовища СТІ шляхом його декомпозиції на інформаційні та функціональні компоненти. Це відкриває шлях до ідентифікації всіх компонентів, визначення їх властивостей (семантики інформації та особливості носія інформації, сутність перетворень інформації (передача, копіювання, зберігання, принципи інтеграції семантик, локального аналізу, класифікації та інше). В свою чергу, до кожного інформаційного процес також може бути застосована аналогічна декомпозиція. Ітеративна декомпозиція до необхідного рівня деталізації дозволяє формалізовано описувати складне інформаційне середовище у вигляді ієрархічної структури.

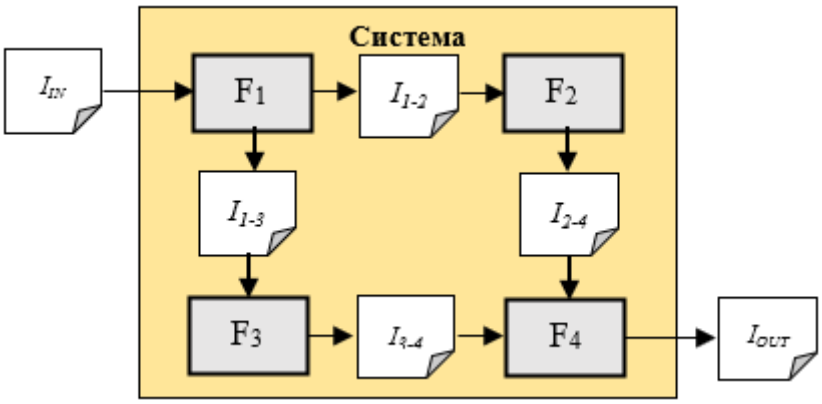


Рисунок 1 – Інформаційно-функціональна структура системи

**2. Метод семантичного синтезу базових понять.** Вербальний опис процесів у сферах кіберзахисту та розвідки кіберзагроз часто супроводжується семантичною невизначеністю. Найбільш поширено таки невизначеності формуються за рахунок підміни понять: *кіберзагроза* замінюються на *загрозу* іншому об'єкту; *ідентифікація кіберзагрози* – на *визначення (детектування) кібератаки*; *загроза* – на *ризик загрози* [6], [9], [12].

Інший напрямок формування невизначеностей – пояснення сенсу (семантики) поняття за допомогою термінів, які самі пояснюються через це поняття. Наприклад, дуже часто поняття *інформація* пояснюється через *відомості, дані, знання* або інші поняття, які в свою чергу, пояснюються через *інформацію*. Ланцюжок таких понять в семантичних мережах створює "замкнуте коло", яке формує багато проблем для наукових досліджень та синтезу інформаційних технологій. З метою подолання цих проблем у подальшому будемо використовувати наступні інструменти формалізації.

*Поняття* (концепт) – це уявна конструкція, яка поєднує наступні частини:

1) *термін* (ідентифікатор поняття) – це слово, або словосполучення за яким ідентифікується (позначається) об'єкт, явище або процес;

2) *визначення* (семантика або сенс поняття) – це упорядкований за правилами мови набір слів (термінів), що пояснює сенс поняття.

Формалізовано структура "поняття" може бути пояснена наступною формулою:

$$\text{"поняття"} = \text{"ідентифікатор поняття" (або термін)} = \{\text{термін}_1, \text{термін}_2, \ldots \text{термін}_N\}, \quad \text{"семантика поняття" (або сенс, визначення)} \tag{7}$$

Відповідно до представлення (7) можна стверджувати, що *визначення (семантика, сенс, сутність) поняття* – це упорядкований за правилами мови набір інших термінів.

Для забезпечення досліджень на основі вказаного підходу було розроблено вимоги до формування професійних понять у сфері забезпечення кібербезпеки та розвідки кіберзагроз:

– не використовуються невизначені поняття;

– нові поняття визначаються за допомогою базових понять та раніше визначених понять;

– до набору базових понять відносяться входять тільки ті, що узгоджені між собою за сенсом (тобто, в рамках набору не створюється "замкнуте коло");

– необхідні нові поняття формуються за допомогою базових та раніше визначених понять (тобто, не застосовуються невизначені професійні поняття).

Наприклад, для визначення поняття *кіберпростір* було використано наступний набір базових понять, що з'явився за результатами аналізу складових інформаційної системи (ІС) [13].

*Інформація про об'єкт $A$ в об'єкті $B$*, $I(A:B)$ – це властивість (атрибут) об'єкту $B$, що придбана (перенесена) в результаті фізичної взаємодії з об'єктом $A$ та є відображенням властивості цього об'єкту $A$.

*Носій інформації* – об'єкт, в якому відображені властивості іншого об'єкту.

*Користувач ІС* – це людина або технічний об'єкт (система), які використовують інформаційний продукт ІС в своїх інтересах (цілях).

*Інформаційний продукт ІС* – це інформація із заданими користувачем властивостями, яка формується інформаційним сервісом (послугою).

*Інформаційний сервіс* (послуга) – це сукупність дій з вхідною інформацією, що формує інформаційний продукт із заданими властивостями.

*Властивості інформації* – це ті якості інформації, які потрібні користувачеві інформації (конфіденційність цілісність, доступність, актуальність достовірність та інші).

*Інформаційне відношення* – це сукупність вхідної інформації, обраного інформаційного сервісу та сформованого інформаційного продукту.

За допомогою цього набору було визначено поняття *кіберпростір ІС* та *кібербезпека ІС*.

*Кіберпростір ІС* – це сукупність інформаційних відносин між користувачами ІС, які формуються за допомогою комп'ютерних послуг (сервісів) цих систем;

*Кібербезпека ІС* – це стан інформаційної системи, при якому навмисні несанкціоновані дії у кіберпросторі не порушують для користувачів послуг задані властивості інформації.

Ці поняття у подальшому будуть використані в якості основи для формування базового набору узгоджених понять для сфери розвідки кіберзагроз.

**3. Базовий набір узгоджених понять для розвідки кіберзагроз.** З метою подальшого уточнення сутності процесів розвідки кіберзагроз на основі отриманого набору взаємозв'язаних понять *інформаційній сервіс, кіберпростір* та *кібербезпека* було сформовано наступне твердження відносно сутності інформаційної системи:

> *Інформаційна система може бути розглянута як сукупність інформаційних сервісів, кожний з яких реалізований за допомогою конкретних комп'ютерних компонент такої системи.*

Таке твердження дозволяє за допомогою методу ССБП сформувати наступний базовий набір узгоджених понять для СТІ.

*Активи ІС* – це компоненти ІС (апаратні та програмні комп'ютерні засоби, персонал, інформаційні ресурси (файли, трафіки, обчислювальні процеси, ланцюжки поставки послуг та інше), що задіяні в реалізації *інформаційних сервісів*.

*Вразливість ІС* – це така властивість *активу ІС*, що може бути використана зловмисником для порушення *кібербезпеки*.

*Кіберзагроза (далі – загроза)* – це можливі дії зловмисника відносно вразливості щодо порушення *кібербезпеки*.

*Ризик загрози* – це характеристика загрози, що залежить від ймовірності її реалізації та прогнозованого збитку.

*Оцінка ризику загрози* – це значення (кількісне або якісне, об'єктивне або суб'єктивне) ризику загрози.

*Кібератака* – це реалізована загроза, або загроза в стадії реалізацій.

*Кіберзахист* – сукупність дій щодо забезпечення стану кібербезпеки.

Семантика сформованого набору понять відображає основну послідовність дій в процесі підготовки та реалізації зловмисного втручання в інформаційну систему. Це може бути використано для подальшого визначення ролі розвідки кіберзагроз в процесі кіберзахисту.

**4. Функція розвідки кіберзагроз в процесі кіберзахисту.** Формалізовано розвідку кіберзагроз можна представити у вигляді інформаційного процесу, що є частиною процесу кіберзахисту. Для такого представлення було застосовано графічний опис інформаційних процесів у вигляді *інформаційно-функціональної структури* (ІФС, рис. 1) та набір наступних моделей для сфери кіберзахисту:

a) Цикл керування кібербезпекою, ЦКК [15], [16];

b) Ланцюжок кіберзнищення *(Cyber Kill Chain, CKC*) [17], [18];

c) Модель чотирьох інформаційних середовищ кібератаки (model of four CyberAttack Information Environments, далі – 4CAIE) [19].

В рамках моделі ЦКК процес кіберзахисту представлений у вигляді циклічного виконання послідовності з п'яті функцій (рисунок 2):

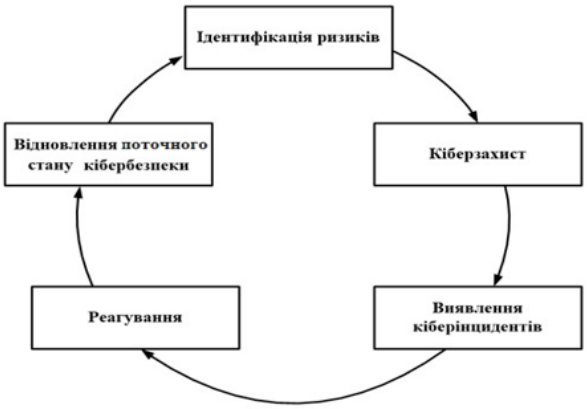


Рисунок 2 – Цикл керування кібербезпекою

Перша функція "Ідентифікація ризиків кібербезпеки" (ID) передбачає заходи, реалізація яких спрямована на поглиблення знань керівництва та персоналу ІС щодо наявних ризиків загроз, їх пріоритетності та способів управління цими ризиками з метою забезпечення надання важливих послуг [16]. Інші функції ЦКК направлені на впровадження необхідних засобів кіберзахисту та реалізацію за їх допомогою відповідних заходів щодо протидії визначеним загрозам.

Така модель дозволяє розглядати розвідку кіберзагроз, як реалізацію функції ID, що забезпечує подальші процеси кіберзахисту інформацією про можливі загрозим та відповідні способи протидії.

Наступна модель *Cyber Kill Chain* формалізує за допомогою спеціалізованого вербального опису дії зловмисника в рамках складних APT атак (англ. *Advanced Persisten Threat* – вдосконала стійка (довготривала) загроза) у вигляді послідовності наступних етапів.

1. *Розвідка* (Reconnaissance) – дослідження, ідентифікація та вибір цілей, збір та аналіз інформації про жертву з відкритих джерел.
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.
3. *Доставка* (Delivery) – передача (проникнення) зброї в комп'ютерне середовище цільової організації.
4. *Експлуатація* (Exploitation) – після того, як зброя доставлена, починається експлуатація вразливостей комп'ютерного середовища цільової організації. Найчастіше експлуатація націлена на вразливість програм, операційної системи або користувачів.
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.

Модель дозволяє за допомогою спеціалізованого вербального опису формувати прогнози про можливі APT атаки на ресурси корпоративної ІС. Недолік цієї моделі – відсутні доступні пояснення про перехід від вербального опису до опису, що зможуть "зрозуміти" комп'ютерні пристрої інфраструктури кіберзахисту.

Найбільш популярна інтерпретація моделі CKC – це модель корпорації Mitre, що застосовує CKC для структурування знань про тактики та прийоми противника. База знань про загрози (фреймворк) MITRE ATT&CK дозволяє детально прогнозувати поведінку зловмисника за допомогою широко відомого концепту як тактики, техніки та процедури (Tactics, Techniques, Procedures, далі – TTPs) [18].

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.

2. *Техніки* (прийоми, T) представляють собою набір заходів, за допомогою яких противник досягає тактичної мети.

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). Таким чином, ресурси MITRE ATT&CK дозволяють аналітикам CTI формувати деталізовані карти атаки (attack map) на основі технічних відомостей про TTPs. 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.

Розвитком підходу формалізації процесів розвідки кіберзагроз є модель 4CAIE, розроблена на основі парадигми ATNI. Структура моделі представлена на рисунку 3. 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 ней. 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).

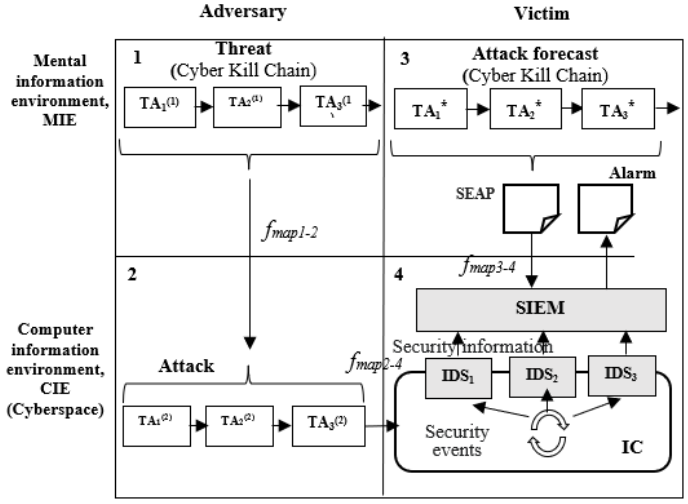


Рисунок 3 – Модель 4-х інформаційних середовищ кібератаки (4CIE)

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 інформаційної системі. В сегменті відображаються впливи атаки противника та дії жертви щодо кіберзахисту від цієї атаки (далі, сегмент кіберзахисту).

В моделі показані інформаційні зв'язки між сегментами, які можна представити операторами інформаційного вплив:

1) $f_{map1-2}$ – оператор, що дозволяє перетворювати семантичні конструкції MIE в конструкції CIE. Реалізується людиною шляхом маніпулювання комп'ютерними засобами вводу-виводу даних (тобто, використовується людино-машинний інтерфейс). Цей оператор показує як *загроза*, що була сформована в ментальному просторі зловмисника перетворюється в конкретну *атаку* в його комп'ютерному середовищі;

2) $f_{map2-4}$ – оператор, 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. Тобто дії в сегменті 2 (*атака*) відображаються в реактивні дії в комп'ютерної системи жертви;

3) $f_{map3-4}$ – оператор інформаційного впливу, що дозволяє по аналогії з $f_{map1-2}$ перетворювати семантичні конструкції MIE команди захисників (тобто, *Attack forecasts – прогнози атак*) в конструкції CIE (шаблони індикаторів компрометації (SEAP) для засобів SIEM). Тобто цей сегмент можна віднести до розвідки загроз.

Представлені формалізми дозволяють сформувати наступну модель ролі розвідки кіберзагроз в процесі кіберзахисту (рисунок 4, таблия 1).

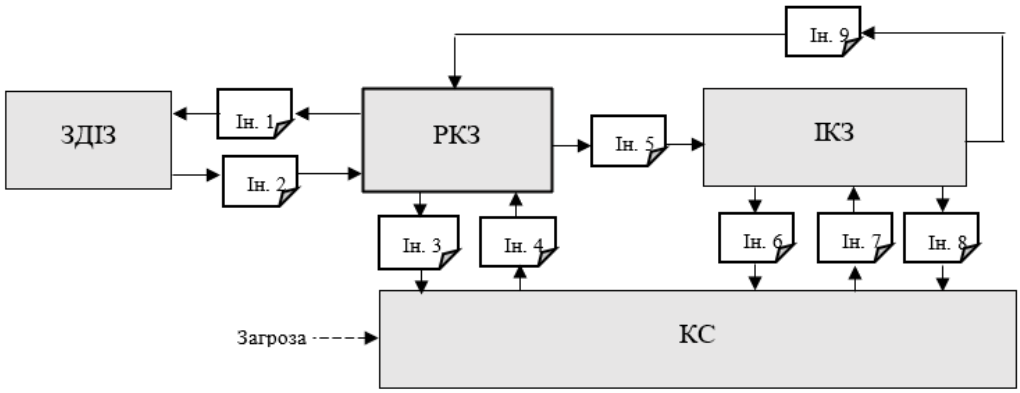


Рисунок 4 – Модель ролі (функції) розвідки загроз в процесі кіберзахисту

В рамках циклу керування кібербезпекою інформаційної системи CTI виконує функцію "Ідентифікацію ризиків кіберзагроз" (ID) наступним шляхом:

– пошук (Ін.1) та збір (Ін.2) інформації про можливі загрози з зовнішніх джерел;

– пошук (Ін.3) та збір (Ін.4) інформації про можливі вразливості КС (шляхом перевірки на проникнення, дозволяє визначити релевантні загрози з загального переліку);

– формування розвідувального продукту (Ін. 5);

– впровадження даних розвідувального продукту в процеси кібкрзахисту (функція “Кіберзахист” ЦКК);

– детектування інцидентів безпеки (Ін. 7) за допомогою розвідувального продукту та формування ІКЗ параметрів реакції на інциденти кібербезпеки для відновлення стану безпеки КС (функції 3-5 ЦКК: “Виявлення (детектування) інцидентів безпеки”, “Реагування на інцидент безпеки”, “Відновлення стану кібербезпеки”);

– інформування РКЗ про поточний стан кібербезпеки по всім опрацьованим загрозам (Ін.9, можлива форма – *поточний профіль захисту*) [19].

Таблиця 1 – Компоненти моделі

| № | Код | Назва |
|---|---|---|
| | | *Функціональні компоненти структури* |
| 1 | КС | Комп’ютерна система |
| 2 | ІКЗ | Інфраструктура кіберзахисту |
| 3 | РКЗ | Розвідка кіберзагроз |
| 4 | ЗДІЗ | Зовнішні джерела інформації про загрози |
| | | *Інформація* |
| 1 | Ін. 1 | Параметри пошуку загроз |
| 2 | Ін. 2 | Інформація про загрози |
| 3 | Ін. 3 | Параметри пошуку вразливостей КС |
| 4 | Ін. 4 | Інформація про вразливості КС |
| 5 | Ін. 5 | Розвідувальний продукт |
| 6 | Ін. 6 | Індикатори компрометації загрози |
| 7 | Ін. 7 | Інформація про події безпеки |
| 8 | Ін. 8 | Параметри реакції на інциденти кібербезпеки |
| 9 | Ін. 9 | Інформація про поточний стан кібербезпеки |

Примітка:

1. Послідовність інформаційних процесів відповідає зростанню номерів в кодах інформації.

2. Інфраструктура кіберзахисту – сукупність організаційно-технічних заходів з кіберзахисту.

Запропонована модель дозволила деталізувати роль (функцію) СТІ в процесах кіберзахисту ІС та класифікувати супутню інформацію про кіберзагрози. Може бути використана як для розробки алгоритмів відповідних програмних технологій, так і для локалізованого аналізу можливих варіантів використання ШІ в процесах захисту.

**5. Інформаційні процеси розвідки кіберзагроз.** Модель функції розвідки загроз в процесі кіберзахисту (рис. 4) не розкриває сутність внутрішніх процесів. Тобто, розвідка була представлена у вигляді “чорної скриньки”. Додаткова модель (рисунок 5), що розроблена за допомогою методу структурного аналізу інформаційних середовищ (САІС), конкретизує ці процеси та їх організацію, дозволяє класифікувати внутрішню інформацію. Кожний інформаційний процес $IP_n$ складається з вхідної інформації $I_{in}^{(n)}$, її перетворення $F_m^{(n)}$ та вихідної інформації $I_{out}^{(n)}$ (6). В межах інформаційно-функціональної структури вихідна інформація одного процесу є вхідною інформацією наступного.

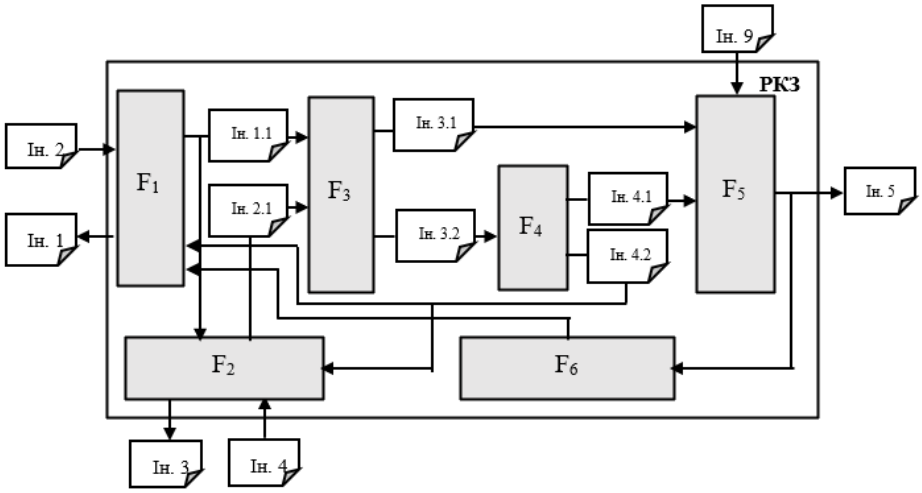


Рисунок 5 – Модель інформаційних процесів розвідки кіберзагроз

Таблиця 2 – Компоненти моделі процесів

| № | Код | Назва |
|---|---|---|
| | | *Функціональні компоненти структури* |
| 1 | $F_1$ | Пошук та збір інформації про загрози з зовнішніх джерел |
| 2 | $F_2$ | Пошук та збір інформації про актуальні вразливості КС (тестування на проникнення) |
| 3 | $F_3$ | Перевірка на релевантність актуальним вразливостям КС, достовірність, актуальність та повноту. |
| 4 | $F_4$ | Аналіз |
| | $F_5$ | Формування розвідувального продукту |
| | $F_6$ | Архівація. |
| | | *Інформація структури* |
| 1 | Ін. 1 | Параметри пошуку загроз |
| 2 | Ін. 2 | Інформація про загрози від зовнішніх джерел |
| 3 | Ін. 3 | Параметри пошуку актуальних вразливостей КС |
| 4 | Ін. 4 | Інформація про актуальні вразливості КС |
| 5 | Ін. 1.1. | Результати збору: перелік загроз та відповідні матеріали про загрози |
| 6 | Ін. 2.1. | Інформація про актуальні вразливості КС |
| 7 | Ін. 3.1. | Інформація, що відповідає критеріям |
| 8 | Ін. 3.2. | Інформація, що не відповідає критеріям |
| 9 | Ін. 4.1. | Інформація, що відповідає критеріям аналізу |
| | Ін. 4.2. | Параметри пошуку додаткової інформації про загрози |
| | Ін. 4 | Розвідувальний продукт |

Опис процесів.

***IP1***: за параметрами пошуку *Ін.1* з відкритих зовнішніх джерел збирається актуальна інформація про загрози *Ін.2.* На її основі $F_1$ формує результати збору *Ін.1.1* (це кодифікований перелік загроз та відповідні матеріали про загрози).

***IP2***: за результатами тестування на проникнення комп'ютерної системи ($F_2$) формується інформація про актуальні вразливості КС *Ін.1.2.*

***IP3***: на основі *Ін.1.3* та *Ін.1.2* формуються ($F_3$) результати збору, що відповідають критеріям релевантності актуальним вразливостям КС, достовірність, актуальність та повноту,

(*Ін.3.1)* та не відповідають (*Ін.3.2)*. *Ін.3.1* безпосередньо поступає на функцію формування розвідувального продукту ( $F_5$ ).

***IP₄***: інформація *Ін.3.2* аналізується ( $F_4$ ) на предмет невідповідності критеріям $F_3$. За результатами формуються додаткові запити на отримання уточнюючий інформації про загрози та вразливості *Ін.4.2.* У разі позитивного уточнення формується інформація по відповідним загрозам *Ін.4.1.*

***IP₅***: на основі матеріалів інформації *Ін.3.1*, *Ін.4.1* та результати впровадження в інфраструктуру кіберзахисту поточного профілю захисту (*Ін.9*) формується ( $F_3$ ) розвідувальний продукт *Ін.5*. Продукт може бути у вигляді цільового профілю захисту [15], [16], в якому відображаються:

- актуальні вразливості конкретних компонентів КС та пов'язані з ними загрози;
- оцінки ризиків загроз;
- TTP та індикатори компрометації по кожній загрозі;
- додаткові заходи захисту щодо обробки ризиків загроз;
- пропозиції щодо впровадження запропонованих заходів захисту.

**6. Практичне застосування запропонованих моделей/** За допомогою запропонованих моделей на основі реляційної бази даних була створена *Система керування інформацією розвідки кіберзагроз (СКІ РКЗ)*. Для формалізації завдання щодо розробки була розроблена наступна концепція системи:

**1) Загальний опис ситуації**

1.1. Корпоративна інформаційна система розглядається як сукупність *інформаційних сервісів* (IS).

1.2. Кожний IS пов'язаний з конкретним:

a) комп'ютерним забезпеченням (апаратним та програмним);

b) персоналом (клієнтом сервісу):

c) мережевим трафіком між комп'ютерними засобами інформаційної системи;

d) до інформації кожного IS задаються вимоги відносно забезпечення властивостей (К, Ц, Д, або інші).

e) забезпечення заданих властивостей для всіх IS в умовах зловмисних впливів на інформаційну – завдання інфраструктури кіберзахисту.

1.3. Загроза кібербезпеки інформаційній системі (далі – загроза) розглядається як сукупність:

a) а) вразливості (властивості компонент інформаційної системі, що дозволяють зловмиснику порушити стан кібербезпеки );

b) б) та можливих дій зловмисника (ДЗ) відносно кожної вразливості.

1.4. Всі вразливості пов'язані з конкретними компонентами інформаційної системи (апаратне та програмне забезпечення КС, інформаційні ресурси (файли, папки директорії), персонал, ланцюжки поставок обладнання та інше).

1.5. Загроза в стадії реалізації, або реалізована загроза, розглядаються як *атака*.

1.6. Розглядаються тільки зовнішні загрози, що можуть буди реалізовані через транспортні сервіси Інтернет.

1.7. Для забезпечення стійкості до кібератак в рамках інформаційної системи створена *інфраструктура кіберзахисту* (ІКЗ), яка функціонує на основі циклу керування кібербезпекою [15], [16].

1.8. Для забезпечення роботи ІКЗ впроваджується служба розвідки кіберзагроз (CTI).

**2) Завдання РКЗ:**

- ідентифікація ресурсів інформаційної системи, властивості яких можуть бути використані в рамках загрози;
- формування та підтримка актуального реєстру ресурсів:
- ідентифікація актуальних загроз на основі інформації доступних джерел;

– формування та підтримка актуального реєстру загроз;
– оцінювання ризиків загроз для корпорації (за технологією SCAP);
– аналіз тактик, технік та процедур (концепція TTP), визначення заходів протидії та індикаторів компрометації);
– прийняття рішення щодо необхідності обробки загрози;
– підготовка пропозицій щодо заходів обробки загрози.

**3) Основні завдання СКІ РКЗ:**

– підтримка реєстру ресурсів;
– підтримка реєстру загроз (ідентифікатори, опис, ТТЗ, оцінки ризиків загроз, пропозиції щодо обробки, відповідальні, результати обробки, дати);
– підтримка реєстру ресурсів ІКЗ;
– автоматизоване формування поточного та цільових профілей захисту.

Реалізація концепції проводилась на основі відомої класифікації заходів кіберзахисту платформи *Framework for Improving Critical Infrastructure CyberSecurity (CSF)* [15], [16]. Реєстр актуальних активів інформаційної системи сформований сукупністю таблиць відповідно до наступних категорій класу заході кіберзахисту "Ідентифікація ризиків кібербезпеки" (ID):

*ID.AM-1.* Апаратне обладнання та системи;
*ID.AM-2.* Програмне забезпечення;
*ID.AM-3.* Комунікаційні потоки даних (трафіки);
*ID.AM-4.* Зовнішні інформаційні та інформаційно-комунікаційні системи;
*ID.AM-5.* Критичность бізнес-процесів та їх активів.

Всі ці таблиці поєднані за допомогою таблиці *Загрози (реєстр загроз),* в якій відображається наступна інформація:

– код загрози;
– семантичний ідентифікатор;
– дата реєстрації;
– короткий опис;
– пов'язані активи;
– оцінка ризику загрози;
– посилання на розширений внутрішній опис загрози;
– посилання на зовнішні джерела;
– стадія обробки загрози РКЗ ( $F_2 - F_5$ , рис. 5):
– коди TTP;
– індикатори компрометації;
– стадії впровадження інформації в інфраструктуру кіберзахисту (етапи 2-5, рис. 1).

На основі сформованих реєстрів система дозволяє за завданими параметрами автоматизовано формувати поточний та цільовий профілі захисту.

Розроблена СКІ РКЗ дозволяє створювати електронні реєстри інформації розвідки кіберзагроз та автоматизувати її обробку. Орієнтована на застосування в рамках SOC корпоративних інформаційних систем.

**Висновки.** Високий рівень невизначеностей у опису розвідки кіберзагроз, що значно затрудняє впровадження класичних технологій автоматизації, оцінювання їх необхідності та ефективності. Відсутність конкретики в розумінні інформаційних процесів також заважає впровадженню засобів штучного інтелекту: складно визначити місце застосування та принципову можливість навчання нейронної мережі на даних розвідки кіберзагроз.

З метою подолання цієї проблеми в рамках досліджень на основі парадигми атрибутивна-трансферного підходу до природи інформація, засобів системного та семантичного аналізу були розроблені *метод структурного аналізу інформаційних процесів* та *метод семантичного синтезу базових понять*. Використання цих методів дозволило сформувати:

- базовий набір узгоджених понять розвідки кіберзагроз;
- модель ролі (функції) розвідки загроз в процесі кіберзахисту;
- модель інформаційних процесів розвідки кіберзагроз.

Результати досліджень дозволяють представити розвідку кіберзагро у вигляді сукупності (інформаційно-функціональної структури) узгоджених інформаційних процесів. Для кожного з цих процесів визначена семантика інформації та сутність її перетворень. З метою подальшого уточнення до потрібного рівня конкретизації кожний з процесів також може бути представлений інформаційно-функціональної структурою. Запропоновані моделі дозволяють класифікувати інформацію розвідки загроз та формувати структури для її інтеграції в рамках запровадження класичних автоматизованих технологій обробки. Значно спрощується процедура аналізу можливості застосування технологій штучного інтелекту.

За результатами досліджень розроблена комп'ютерна система для підтримки процесів керування ризиками кіберзагроз корпоративної інформаційної системи. Система орієнтована на застосування в рамках SOC.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ


[1] G. Johansen, *Digital Forensics and Incident Response. An intelligent way to respond to attacks*. Birmingham, UK, 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, Wiley Online Library, 2019, pp. 1-49. 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] "What is Threat Intelligence?", *Broadcom*, 2023. [Online]. Available: https://www.vmware.com/topics/glossary/content/threat-intelligence.html. Accessed on: June 20, 2023.

[5] C. Johnson, L. Badger, D. Waltermire, J., Snyder, and C. Skorupka, *NIST Special Publication 800-150, Guide to Cyber Threat Information Sharing*. USA: NIST, 2016. doi: http://dx.doi.org/10.6028/NIST.SP.800-150.

[6] P. Santos, R. Abreu, M.J.C.S. Reis, C. Serôdio, and F. Branco, "A Systematic Review of Cyber Threat Intelligence: The Effectiveness of Technologies, Strategies, and Collaborations in Combating Modern Threats", Sensors, vol. 25 (14), art. 4272, 28 p., 2025. doi: https://doi.org/10.3390/s25144272.

[7] Y. Guo, Z. Liu, C. Huang, N. Wang, H. Min, W. Guo, and Liu, J., "A framework for threat intelligence extraction and fusion", *Comput. Secur*, vol. 132, art. 103371, 2023. doi: https://doi.org/10.1016/j.cose.2023.103371.

[8] P. Gao, F. Shao, X. Liu, X. Xiao, Z. Qin, F. Xu, P. Mittal, S.R. Kulkarni, and D. Song, "Enabling Efficient Cyber Threat Hunting with Cyber Threat Intelligence", in *Proc. IEEE 37th Int. Conf. on Data Engineering (ICDE)*, Chania, Greece, 2021, pp. 193-204. doi: https://doi.org/10.48550/arXiv.2010.13637.

[9] S. El Jaouhari, Y.I: Etiabi, Federated Learning and Cyber Threat Intelligence on the Edge for secure IoT Networks, in *Proc. Int. Conf. Internet of Things* (*IoT 2023*), Nagoya, Japan, 2023, pp. 98-104. doi: https://doi.org/10.1145/3627050.3627064.

[10] L.F. Sikos, "Cybersecurity knowledge graphs", *Knowledge and Information Systems*, vol. 65, pp. 3511-3531, 2023. doi: https://doi.org/10.1007/s10115-023-01860-3.

[11] J. Trivedi, M. Tahir, and J. Isoaho, "AI-Enhanced Threat Intelligence in Remote Patient Monitoring Systems: A Survey on Recent Advances, Challenges and Future Research Directions", *IEEE Access*, vol. 13, art. 20540, pp. 106465-106488. doi: https://doi.org/10.1109/ACCESS.2025.3572626.

[12] I. Yakoviv, "Information, signs, knowledge and intelligence", *Information Technology and Security*, вип. 8, т. 2 (15), pp. 191-215, 2020. doi: https://doi.org/10.20535/2411-1031.2020.8.2.222605.
[13] А.Б. Качинський, *Безпека, загрози і ризики: наукові концепції та математичні методи*. Київ, Україна: НА СБУ, 2004.
[14] І. Яковів, "Інформаційно-телекомунікаційна система, концептуальна модель кіберпростору і кібербезпека", *Information Technology and Security*, вип. 5, т. 2, с. 134-144, 2017. doi: https://doi.org/10.20535/2411-1031.2017.5.2.136981.
[15] *Framework for Improving Critical Infrastructure Cybersecurity*. *ver. 1.0*. USA: NIST, 2014. [Online]. Available: https://www.nist.gov/system/files/documents/cyberframework/cybersecurity-framework-021214.pdf. Accessed on: Sep. 25, 2025.
[16] 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.
[17] 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 Co.*, 14 p., 2014. [Online]. Available: https://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf. Accessed on: Sep. 29, 2025.
[18] B.E. Strom, A. Applebaum, D.P. Miller, K.C. Nickels, A.G. Pennington, and C.B. Thomas, *MITRE ATT&CK: Design and Philosophy*. The MITRE Corporation, 2020
[19] І. Яковів, "Модель чотирьох інформаційних середовищ кібератаки", *Information Technology and Security*, вип. 5, т. 2 (21), с. 176-192, 2023. doi: https://doi.org/10.20535/2411-1031.2023.11.2.293768.

Стаття надійшла до редакції 02.11.2025.

## REFERENCE

[1] G. Johansen, *Digital Forensics and Incident Response. An intelligent way to respond to attacks*. Birmingham, UK, 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, Wiley Online Library, 2019, pp. 1-49. 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] "What is Threat Intelligence?", *Broadcom*, 2023. [Online]. Available: https://www.vmware.com/topics/glossary/content/threat-intelligence.html. Accessed on: June 20, 2023.
[5] C. Johnson, L. Badger, D. Waltermire, J., Snyder, and C. Skorupka, *NIST Special Publication 800-150, Guide to Cyber Threat Information Sharing*. USA: NIST, 2016. doi: http://dx.doi.org/10.6028/NIST.SP.800-150.
[6] P. Santos, R. Abreu, M.J.C.S. Reis, C. Serôdio, and F. Branco, "A Systematic Review of Cyber Threat Intelligence: The Effectiveness of Technologies, Strategies, and Collaborations in Combating Modern Threats", Sensors, vol. 25 (14), art. 4272, 28 p., 2025. doi: https://doi.org/10.3390/s25144272.
[7] Y. Guo, Z. Liu, C. Huang, N. Wang, H. Min, W. Guo, and Liu, J., "A framework for threat intelligence extraction and fusion", *Comput. Secur*, vol. 132, art. 103371, 2023. doi: https://doi.org/10.1016/j.cose.2023.103371.
[8] P. Gao, F. Shao, X. Liu, X. Xiao, Z. Qin, F. Xu, P. Mittal, S.R. Kulkarni, and D. Song, "Enabling Efficient Cyber Threat Hunting with Cyber Threat Intelligence", in *Proc. IEEE 37th*

*Int. Conf. on Data Engineering (ICDE)*, Chania, Greece, 2021, pp. 193-204. doi: https://doi.org/10.48550/arXiv.2010.13637.
[9] S. El Jaouhari, Y.I: Etiabi, Federated Learning and Cyber Threat Intelligence on the Edge for secure IoT Networks, in *Proc. Int. Conf. Internet of Things* (*IoT 2023*), Nagoya, Japan, 2023, pp. 98-104. doi: https://doi.org/10.1145/3627050.3627064.
[10] L.F. Sikos, "Cybersecurity knowledge graphs", *Knowledge and Information Systems*, vol. 65, pp. 3511-3531, 2023. doi: https://doi.org/10.1007/s10115-023-01860-3.
[11] J. Trivedi, M. Tahir, and J. Isoaho, "AI-Enhanced Threat Intelligence in Remote Patient Monitoring Systems: A Survey on Recent Advances, Challenges and Future Research Directions", *IEEE Access*, vol. 13, art. 20540, pp. 106465-106488. doi: https://doi.org/10.1109/ACCESS.2025.3572626.
[12] I. Yakoviv, "Information, signs, knowledge and intelligence", *Information Technology and Security*, vol. 8, iss. 2 (15), pp. 191-215, 2020. doi: https://doi.org/10.20535/2411-1031.2020.8.2.222605.
[13] A.B. Kachynsky, *Security, Threats and Risks: Scientific Concepts and Mathematical Methods*. Kyiv, Ukraine: NA SSU, 2004.
[14] I. Yakoviv, "Information and telecommunications system, conceptual model of cyberspace and cybersecurity", *Information Technology and Security*, vol. 5, iss. 2, pp. 134-144, 2017. doi: https://doi.org/10.20535/2411-1031.2017.5.2.136981.
[15] *Framework for Improving Critical Infrastructure Cybersecurity*. *ver. 1.0*. USA: NIST, 2014. [Online]. Available: https://www.nist.gov/system/files/documents/cyberframework/cybersecurity-framework-021214.pdf. Accessed on: Sep. 25, 2025.
[16] Administration of the State Service for Special Communications. (2021, Oct. 06). Order no. 601, *On approval of Methodological recommendations for increasing the level of cyber protection of critical information infrastructure*. [Online]. Available: https://cip.gov.ua/ua/news/nakaz-ad-2021-10-06-601.
[17] 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 Co.*, 14 p., 2014. [Online]. Available: https://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf. Accessed on: Sep. 29, 2025.
[18] B.E. Strom, A. Applebaum, D.P. Miller, K.C. Nickels, A.G. Pennington, and C.B. Thomas, *MITRE ATT&CK: Design and Philosophy*. The MITRE Corporation, 2020
[19] I. Yakoviv, "A Model of Four Information Environments of Cyberattacks", *Information Technology and Security*, vol. 11, iss. 2 (21), pp. 176-192, 2023. doi: https://doi.org/10.20535/2411-1031.2023.11.2.293768.

IGOR YAKOVIV,
DMITRO SHARADKIN,
VASYL KULIKOV

**CYBER THREAT INFORMATION INTELLIGENCE INTEGRATION MODELS**

In the context of the constant growth of information on attacks on information systems, the task of increasing the effectiveness of cyber threat intelligence processes is relevant. As a rule, all information accompanying these processes is called cyber threat intelligence information, without dividing it by the essence of a specific process. On the other hand, the description of the structure of the complex of all processes is very general. All this leads to a high level of uncertainty in the description of cyber threat intelligence, which significantly complicates the implementation of classical automation technologies, assessing their necessity and effectiveness. The lack of specificity in understanding information processes also hinders the implementation of artificial intelligence tools: it is difficult to determine the place of application and the fundamental possibility of training a neural network on cyber threat intelligence data.

One of the directions of overcoming this problem can be the use of formalized constructions that describe the relationship between the main components of the process of formation and application of an intelligence product. As part of the research based on the paradigm of the attributive-transfer approach to the nature of information, means of system and semantic analysis, *a method of structural analysis of information processes* and *a method of semantic synthesis of basic concept*s were developed. The use of these methods allowed to form:

- a basic set of agreed concepts of cyber threat intelligence;
- a model of the role (function) of threat intelligence in the process of cyber defense;
- a model of cyber threat intelligence processes.

The research results allow us to present cyber threat intelligence as a set (information-functional structure) of coordinated information processes. For each of these processes, the semantics of information and the essence of its transformations are defined. In order to refine to the required level of specification, each of the processes can also be represented by an information-functional structure. The proposed models allow us to classify threat intelligence information and form structures for its integration within the framework of the introduction of classical automated processing technologies. The procedure for analyzing the possibility of using artificial intelligence technologies is significantly simplified.

Based on the research results, a computer system was developed to support the processes of managing cyber threat risks in a corporate information system.

**Keywords:** cyber threat intelligence, cyber defense infrastructure, information and functional structure, nature of information, information processes, information integration, intelligence product, synthesis of concepts, artificial intelligence, automation.

**Яковів Ігор Богданович**, кандидат технічних наук, доцент, доцент кафедри комп'ютерних наук та технологій штучного інтелекту у сфері кібербезпеки, 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.

**Шарадкін Дмитро Михайлович**, кандидат технічних наук, доцент, доцент кафедри комп'ютерних наук та технологій штучного інтелекту у сфері кібербезпеки, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна, ORCID ID: 0000–0001–6407–8040, dmsh@ukr.net.

**Куліков Василь Михайлович**, кандидат технічних наук, доцент, доцент кафедри комп'ютерних наук та технологій штучного інтелекту у сфері кібербезпеки, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна, ORCID 0000-0002-1015-5802, k.v.m@i.ua.

**Yakoviv Ihor**, candidate of technical sciences, associate professor, associate professor at the computer science and artificial intelligence technologies in the field of cybersecurity academic department, Institute of special communication and information protection at the National technical university of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine.

**Sharadkin Dmytro**, candidate of technical sciences, associate professor, associate professor at the computer science and artificial intelligence technologies in the field of cybersecurity academic department, Institute of special communication and information protection at the National technical university of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine.

**Kulikov Vasyl**, candidate of technical sciences, associate professor, associate professor at the computer science and artificial intelligence technologies in the field of cybersecurity academic department, Institute of special communication and information protection at the National technical university of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine.