DOI: 10.58254/viti.9.2026.26.332

УДК 004.853+004.056.5

д-р філософії, доцент Фесьоха В. В. ORCID: 0000-0001-6612-1970 (ВІТІ ім. Героїв Крут)
Легкобит В. С. ORCID: 0000-0002-9118-4188 (ВІТІ ім. Героїв Крут)

МОДЕЛЬ ДВОРІВНЕВОЇ ОРГАНІЗАЦІЇ ЗНАНЬ В ІНТЕЛЕКТУАЛЬНИХ СИСТЕМАХ КІБЕРЗАХИСТУ НА ОНТОЛОГІЧНІЙ ОСНОВІ

У контексті підвищення ефективності управління знаннями в інтелектуальних системах кіберзахисту (ІСК) вирішується завдання організації знань на основі онтології кіберзагроз із використанням таксономій MITRE ATT&CK, MITRE CAPEC та наборів даних від European Repository of Cyber Incidents (EuRepoC). Актуальність зазначеного обумовлена необхідністю оперативної інтеграції зростаючих обсягів отриманих даних про кібератаки з наявним семантичним ядром ІСК. До того ж, існуючі підходи до уніфікації та формалізації гетерогенних даних у домені кіберзахисту не забезпечують оперативної та контрольованої інтеграції нових знань у семантичне ядро повноцінного формування єдиного когерентного, семантично-інтероперабельного простору знань, натомість зосереджені виключно на поверхневій консолідації онтологічних ресурсів окремих постачальників, що супроводжується обмеженою гнучкістю масштабування та високим рівнем абстракції, який ускладнює відображення причинно-наслідкових зв'язків між елементами кіберзагроз. У зв'язку з цим, розроблено модель дворівневої організації знань в ІСК на онтологічній основі. Суть запропонованої моделі полягає у формалізації процесу контрольованої інтеграції динамічних потоків фрагментованих даних з домену кіберзахисту через процедуру контекстної узгодженості між динамічним і статичним рівнями на основі розрахунку комплексного показника готовності кандидатів у знання. Оцінка ефективності застосування запропонованої моделі проводилася шляхом автоматизованого послідовного надходження 36 824 векторів даних з 4 наборів даних (MITRE та EuRepoC). В результаті до онтології було додано 23 830 нових сутностей з середнім показником їх готовності до формалізації 0,76 та загальним показником узгодженості онтології на рівні 99 %, що свідчить про збереження здатності онтології підтримувати формування логічних висновків в межах поточного контексту при істотному збагаченні фактологічного змісту.

Ключові слова: *дані, знання, організація знань, управління знаннями, онтології, кібератаки, кіберзахист, контекстна узгодженість, підтримка прийняття рішень.*

V. Fesokha, V. Lehkobyt. A two-level model of knowledge organization in ontology-based cybersecurity systems

In the context of improving the effectiveness of knowledge management in intelligent cyber defense systems (ICDS), the task at hand is to organize knowledge based on a cyber-threat ontology using the MITRE ATT&CK and MITRE CAPEC taxonomies, as well as datasets from the European Repository of Cyber Incidents (EuRepoC). The relevance of this is driven by the need for rapid integration of the growing volumes of cyberattack data into the existing semantic core of the ICDS. Moreover, existing approaches to the unification and formalization of heterogeneous data in the cybersecurity domain do not ensure the rapid and controlled integration of new knowledge into the semantic core for the full-fledged formation of a single coherent, semantically interoperable knowledge space; but instead focus exclusively on the superficial consolidation of ontological resources from individual vendors, accompanied by limited scalability and a high level of abstraction, which complicates the representation of cause-and-effect relationships between elements of cyber threats. In this regard, a model of a two-level ontology-based knowledge organization in ICDS has been developed. The essence of the proposed model lies in formalizing the process of controlled integration of dynamic streams of fragmented data from the cyber defense domain through a procedure of contextual consistency between the dynamic and static levels based on the calculation of a comprehensive knowledge candidate readiness index. The effectiveness of the proposed model was evaluated through the automated sequential input of 36,824 data vectors from 4 datasets (MITRE and EuRepoC). As a result, 23,830 new entities were added to the ontology with an average formalization readiness index of 0.76 and an overall ontology consistency index of 99%, indicating that the ontology retains its ability to support the formation of logical inferences within the current context while significantly enriching its factual content.

Keywords: *data, knowledge, knowledge organization, knowledge management, ontologies, cyberattacks, cybersecurity, contextual consistency, decision support.*

Вступ. У сучасних умовах стрімкої еволюції способів реалізації кіберзагроз ІСК функціонують в середовищі високої інформаційної ентропії та безперервного надходження нових даних, де традиційні стратегії акумуляції та систематизації досвіду вичерпують свою ефективність. Протягом тривалого часу домінуючим підходом до інтеграції розрізнених даних у домені кіберзахисту був пошук ефективного способу створення універсальної онтології, яка

об’єднала б фізичні, когнітивні та соціальні аспекти кіберпростору [1]. Однак такий підхід часто призводить до теоретичного колапсу та категоріальних помилок, виявляючись надто жорстким для динамічних загроз.

У зв’язку з цим особливої актуальності набуває не лише побудова моделей знань в домені кіберзахисту, а й організація процесів їх формування, оновлення та використання в умовах безперервного надходження даних.

Постановка завдання в загальному вигляді. Організація знань в сучасних ІСК є одним із ключових етапів життєвого циклу управління знаннями, оскільки саме ступінь узгодженості елементів моделі знань забезпечує чітку категоризацію, швидкий пошук і доступ, полегшує інтеграцію, а також сприяє однозначному розумінню та ефективному використанню збережених знань. У контексті зазначеного залишається невирішеним завдання досягнення компромісу між здатністю до своєчасного регулярного оновлення моделі знань ІСК та забезпеченням якості і достовірності знань у процесі прийняття рішень, а також збереженням цілісності та консистентності знань під час їх оновлення, масштабування або трансформації структури моделі знань [2]. Зазначене обумовлює необхідність підвищення адаптивності моделей знань ІСК на онтологічній основі до безперервного надходження гетерогенних даних кіберрозвідки (Cyber Threat Intelligence, CTI) з урахуванням вимог до їхньої якості та достовірності у процесі інтеграції.

Аналіз попередніх досліджень та публікацій [3–14] вказує на необхідність розробки онтологій, що враховують різні аспекти організації та представлення знань у домені кіберзахисту, зокрема важливість інтеграції гетерогенних даних для покращення ситуаційної обізнаності та ефективність застосування когнітивних технологій та технологій штучного інтелекту/машинного навчання порівняно з експертами для вилучення ключових атрибутів предметної області з метою формування комплексного уявлення про поточний ландшафт кіберзагроз.

На сьогодні існує ряд загальнодоступних онтологій (CRATELO, STUCCO, UCO, MALOnt, WAVED Ontology) [3–7], які формують семантичну основу не лише для побудови enterprise CTI/Security Operations Center рішень, а й для проведення наукових досліджень за такими напрямками:

– підвищення рівня кіберситуаційної обізнаності [3–14] – формування цілісного, контекстуального розуміння поточного стану інформаційного середовища, активів, кіберзагроз та вразливостей з метою своєчасного виявлення, оцінювання та прогнозування кіберінцидентів;

– уніфікації гетерогенних даних і забезпечення узгодженого семантичного контексту [3–5; 7; 8; 12; 14] – узгодження, інтеграція та стандартизація даних, отриманих із різнорідних джерел (баз вразливостей, мережевої телеметрії, системи виявлення вторгнень, звітних даних антивірусних систем тощо) у єдиному семантичному просторі з метою створення спільної моделі знань, у межах якої різні типи інформації матимуть єдине визначення, зв’язки та властивості;

– автоматизація вилучення та інтеграція знань [5; 9–11; 14] – автоматичне виявлення, формалізація та об’єднання релевантних фрагментів знань із різних джерел у єдину семантичну модель без участі або з мінімальним втручанням експертів;

– інтеграція принципів організації знань (Knowledge Organization) з технологічними перевагами представлення знань (Knowledge Representation) [3; 4; 7; 12] – поєднання методів систематизації знань, орієнтованих на класифікацію, таксономію та впорядкування понять із формальними технологіями їх подання, що забезпечують машинну обробку, логічне виведення та інтероперабельність;

– підвищення якості моделювання невизначеності [10; 11; 13; 14] – вдосконалення здатності онтологічних систем враховувати неповноту, неоднозначність або відсутність знань про події, об’єкти та зв’язки у сфері кіберзахисту.

Наведений огляд основних напрямків наукових досліджень щодо формалізації знань на онтологічній основі свідчить про значні досягнення у забезпеченні семантичного базису для уніфікації гетерогенних джерел даних для підвищення кіберситуаційної обізнаності. Водночас їх застосування у реальних умовах функціонування інформаційно-комунікаційних систем обмежено відсутністю ефективного механізму узгодження між динамічними потоками даних про кібератаки та статичною онтологічною моделлю знань. Так, у сучасних системах кіберзахисту інтеграція нових знань, як правило, відбувається лише після їх повної верифікації, що призводить до затримок у представленні актуального стану способів реалізації кіберзагроз. З іншого боку, використання сирих або частково оброблених даних без належного семантичного узгодження з існуючою моделлю знань породжує суперечності, знижує якість знань та ускладнює прийняття рішень. До того ж, наразі в галузі кіберзахисту не існує єдиної універсальної онтології, тоді як декілька загальновизнаних моделей знань, стандартів структурованого обміну даними та таксономій використовуються де-факто як онтологічні основи для організації знань у різних піддоменах.

Таким чином, виникає об’єктивне протиріччя між необхідністю оперативного використання динамічних даних з домену кіберзахисту та необхідністю забезпечення їх семантичної узгодженості при інтеграції в онтологічну модель знань.

У зв’язку з цим **метою статті** є розробка моделі організації знань для формалізації поетапної інтеграції даних у онтологію із контролем їх узгодженості в умовах інтенсивного потокового надходження кіберрозвідданих, зберігаючи при цьому повноту доступної для інтерпретації експертом інформації.

Викладення основного матеріалу. Фактичні обмеження метаонтологічних підходів до представлення ландшафту кіберзагроз, зокрема таких як UCO та STUCCO [3; 7], ускладнюють не лише консолідацію гетерогенних даних, представлених у межах спеціалізованих моделей (CAPEC, CVE, CWE, MITRE ATT&CK, STIX) [6; 8], а й забезпечення належного рівня їх семантичної узгодженості та контрольованої інтеграції в єдину модель знань. Основною причиною цього є їх орієнтація на централізовану інтеграцію, що супроводжується обмеженою гнучкістю масштабування та високим рівнем абстракції, який ускладнює відображення причинно-наслідкових зв’язків між елементами кіберзагроз.

У зв’язку з цим доцільним є застосування федеративного підходу, що сформувався в межах розвитку Semantic Web та концепції Ontology alignment [15; 16] і передбачає збереження автономності окремих онтологій при їх узгодженні через систему семантичних відповідностей. Такий підхід забезпечує можливість встановлення коректних відповідностей між концептуально різнорідними сутностями, що надає можливість формувати узгоджений, семантично інтероперабельний простір знань без необхідності повного злиття моделей. На відміну від метаонтологічних реалізацій [3; 7], запропонована модель в кінцевому результаті орієнтована не лише на інтеграцію даних, а й на підтримку аналітичного представлення динаміки способів реалізації кіберзагроз, зокрема через явне врахування взаємозв’язків між кібератаками, вразливостями, цифровими артефактами та механізмами реагування, що є особливо важливим для прийняття рішень в умовах неповноти (фрагментації) інформації.

Архітектура запропонованої моделі передбачає наявність двох рівнів (статичного та динамічного), а також процедури контекстної узгодженості між ними, яка забезпечує прийняття рішень щодо формалізації даних про кібератаки, накопичених на динамічному рівні, як елементів статичної моделі знань (рис. 1).

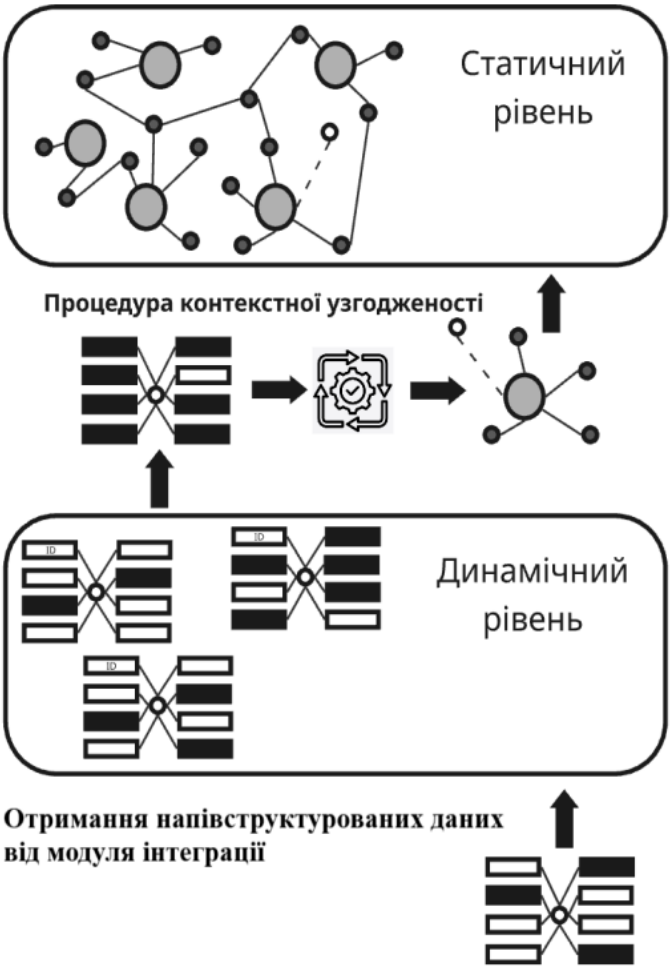

Рис. 1. Узагальнена графічна інтерпретація моделі

Статичний рівень моделі організації знань – федеративна онтологія, що описує домен кіберзахисту, де визначено основні сутності (кампанії, кібератаки, техніки, події тощо), процеси та зв’язки між ними, які у поєднанні формують достатньо повний цикл зловмисної активності у кіберпросторі. Кожному класу статичного рівня відведено специфічну роль у логіко-структурній конфігурації домену, тоді як семантичні зв’язки між ними задають чіткі правила взаємодії, що дає змогу логічно обробляти дані, робити висновки та поєднувати інформацію з різних джерел кіберрозвідки (OpenCTI, OSINT, Dark Web, IoC feeds, CERT, STIX/TAXII тощо). Зазначена онтологія охоплює повний цикл OODA (Observe-Orient-Decide-Act) [17] та побудована на основі підходу, орієнтованого на порушника [18]. На рисунку 2 представлено концептуальну схему статичного рівня моделі організації знань в домені кіберзахисту на онтологічній основі.

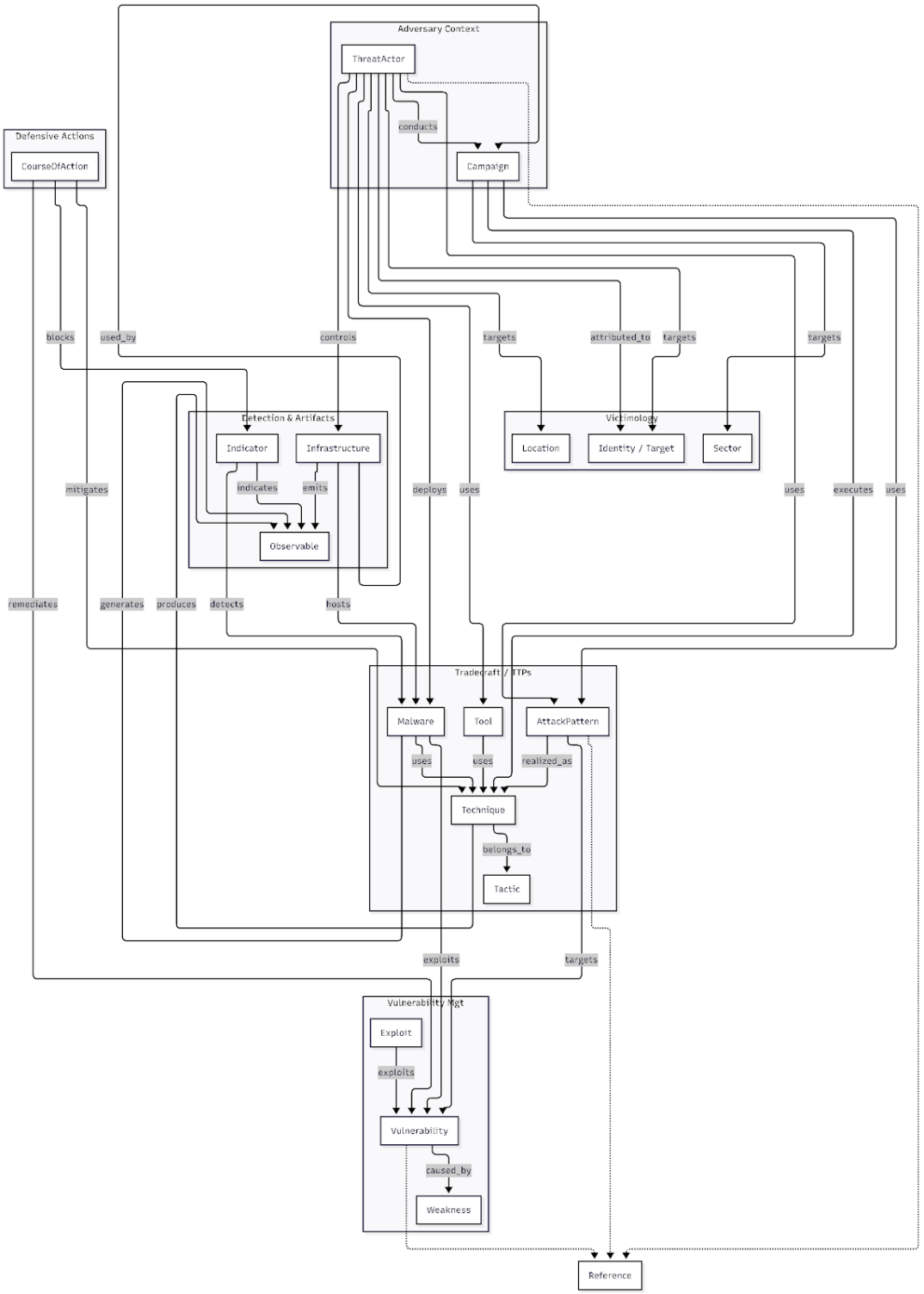

Рис. 2. Концептуальна схема статичного рівня моделі організації знань в домені кіберзахисту на онтологічній основі

У межах статичного рівня моделі концептуальна структура домену кіберзахисту декомпонується на сукупність взаємопов’язаних семантичних піддоменів, кожен з яких відображає окремий аспект загрозливого середовища. Кожен піддомен агрегує класи та відношення, що описують семантично однорідні сутності та їхню взаємодію. Зокрема, піддомен *Adversary Context* охоплює сутності, пов’язані з джерелом кіберзагрози (зловмисник, кампанії), *Tradecraft* – реалізацію кібератак через тактики, техніки та інструменти,

Vulnerability Context – експлуатацію вразливостей, *Detection* – спостережувані артефакти та індикатори, *Victim Context* – характеристики цільових об'єктів, а *Defense* – механізми протидії. Зазначена модульна організація узгоджується з підходами побудови кібербезпекових графів знань, у яких сутності та їх відношення структуруються відповідно до функціональних аспектів домену [19]. В таблиці 1 наведено класи онтології за функціональними групами [3; 5–7; 9; 19].

Таблиця 1

Опис класів онтології статичного рівня

Найменування класу	**Науково-прикладне обґрунтування**
Threat Actor	Центр атрибуції ініціатора цілеспрямованого деструктивного впливу на об'єкти критичної інформаційної інфраструктури
Campaign	Описує стратегічний контекст зловмисної активності через агрегацію відомостей про реалізацію кібератак, спрямованих проти конкретних цілей для досягнення певної мети
Attack Pattern	Абстракція множини технік, що реалізують спільний логічний механізм експлуатації вразливостей системи
Technique	Операційно-процедурна одиниця, яка формалізує конкретні технічні методи реалізації зловмисної активності і слугує точкою конвергенції між її стратегічним плануванням та технічними артефактами
Tactic	Концептуальний елемент ланцюга подій, що структурує життєвий цикл кібератаки
Malware	Програмне забезпечення, спеціально розроблене або модифіковане для порушення конфіденційності, цілісності чи доступності інформаційно-комунікаційних систем
Tool	Формалізує програмні утиліти, комерційні засоби або легітимне програмне забезпечення подвійного призначення, які використовуються зловмисником для підтримки кампаній, але не обов'язково є шкідливими за функціональним призначенням
Infrastructure	Репрезентує матеріально-технічну та технологічну основу забезпечення операційної спроможності проводити кібератаки. З точки зору детекції, інфраструктура є джерелом цифрових артефактів
Observable	Визначає атомарну одиницю цифрової реальності, емпіричний факт, що є продуктом виконання технічних процедур в межах інформаційної інфраструктури
Indicator	Певний набір закономірностей, що формалізує логіку детекції та інтерпретації окремого емпіричного факту як свідчення зловмисної активності
Weakness	Репрезентує фундаментальний рівень абстракції першопричин технічного ризику, які за певних умов можуть призвести до появи вразливостей
Vulnerability	Формалізує сукупність дефектів конкретного програмно-апаратного забезпечення, яка визначає схильність системи до потенційного деструктивного впливу
Exploit	Формалізує активний інструментальний компонент, що використовує вразливості для реалізації деструктивного впливу
Victim Context	Формалізує об'єкти шкідливого впливу та забезпечує стратегічний рівень аналізу загроз через ідентифікацію цілей зловмисника з урахуванням специфічних ризиків для окремих галузей та геополітичної обстановки
Course Of Action	Репрезентує рекомендаційний компонент онтології, спрямований на нейтралізацію загроз та мінімізацію потенційних збитків
Reference	Виконує роль позаієрархічної сутності, що забезпечує епістемологічну цілісність та фактологічну підтримку верифікації знань про кіберзагрози.

Динамічний рівень є операційним каркасом онтології статичного рівня та визначає спосіб перетворення отриманих сирих даних з домену кіберзахисту у формалізовані знання. Так, вхідна інформація про кібератаки в якості кандидатів у формалізовані знання представляється у вигляді множини іменованих підграфів $\{G_1, G_2, \dots, G_n\}$, структура яких узгоджена з класами та відношеннями статичного рівня запропонованої моделі. При цьому підграфи можуть містити неповні, суперечливі або слабоструктуровані дані, що потребують подальшої обробки. Кожен іменований підграф G_i інтерпретується як кандидат на екземпляр відповідного класу онтології та включає фактологічне ядро (сукупність предикатів, що описують сутність та її зв'язки) і метадані (відомості про джерело даних, хронологічні анотації, рівень довіри) з метою подальшого аналізу походження інформації, оцінки її персистентності та забезпечення можливості ретроспективного відстеження змін.

Інтеграція підграфів до статичного рівня здійснюється через комплексну оцінку якості:

– *на рівні предикатів* – перевірка коректності, несуперечливості та семантичної валідності окремих фактів (табл. 2) [20–23];

– *на рівні підграфа* – оцінка структурної цілісності, узгодженості зв'язків та повноти опису (табл. 3) [20–23].

Таблиця 2

Показники якості даних про кібератаки на рівні окремих предикатів

Найменування	**Позначення**	**Практичний сенс**	**Одиниця виміру**	**Референтні значення**
Надійність	r_s	Апріорна оцінка джерела даних, що базується на минулому досвіді	Коефіцієнт (0,0–1,0)	[0,8–1,0] – висока; [0,5–0,7] – середня; < 0,5 – сумнівне джерело
Вірогідність	p_v	Внутрішній статус факту, визначає міру, до якої дані вважаються істинними	Коефіцієнт (0,0–1,0)	[0,9–1,0] – перевірено аналітиком; [0,7–0,9] – технічний факт; [0,5–0,7] – припущення системи
Впевненість	c_p	Апостеріорна оцінка значення предикату, що обчислюється на основі довіри до джерела та міри істинності даних	Коефіцієнт (0,0–1,0)	[0,8–1,0] – висока; [0,5–0,7] – середня; < 0,5 – сумнівний факт
Кардинальність	a_p	Потужність множини унікальних джерел, які надали різні значення предикату	Ціле число	1 – однозначність; > 1 – наявність семантичного конфлікту
Рівень кооборації	k_p	Потужність множини унікальних джерел, які надали ідентичні значення предикату	Ціле число	1 – гіпотеза; > 1 – шлях до консенсусу

Таблиця 3

Показники якості даних про кібератаки на рівні іменованого підграфа

Найменування	**Позначення**	**Одиниця виміру**	**Як враховує рівень предикатів**
Точність семантичної класифікації	A_G	Коефіцієнт (0,0–1,0)	Міра відповідності між значеннями полів вхідного фрагмента даних та формальними обмеженнями предикатів (семантичною сигнатурою) обраного класу онтології статичного рівня
Агрегована впевненість	$Conf_G$	Коефіцієнт (0,0–1,0)	Середньозважене значення впевненості всіх предикатів підграфа
Структурна повнота	$Compl_G$	Коефіцієнт (0,0–1,0)	Відношення фактично заповнених значеннями предикатів до обов'язкового набору предикатів, передбаченого семантичною сигнатурою класу

Найменування	Позначення	Одиниця виміру	Як враховує рівень предикатів
Логічна узгодженість	$Cons_G$	Коефіцієнт (0,0–1,0)	Агрегує показники кардинальності кожного предикату та визначає ступінь потенційного впливу на семантичну цілісність наявної моделі знань
Темпоральна релевантність	T_G	Коефіцієнт (0,0–1,0)	Відображає результат впливу часу на цінність накопичених фактів на рівні предикатів

Для кожного іменованого підграфа G_i передбачено використання унікального ідентифікатора $TYPE_{ID}$, що забезпечує уникнення дублювання даних про кібератаки. Ідентифікатор генерується на основі детермінованого відбору та канонізації значень стабільних предикатів семантичної сигнатури відповідного класу онтології, їх уніфікованої серіалізації та обчислення криптографічної хеш-функції [24].

Семантична сигнатура – це структурована специфікація об'єктних і функціональних властивостей певного класу, яка визначає ступінь відповідності фрагмента вхідних даних екземпляру цього класу. У межах запропонованого підходу кожна семантична сигнатура поділяється на обов'язкові, рекомендовані та опціональні предикати відповідних класів онтології статичного рівня шляхом застосування системи ваг, що надає можливість гнучко оцінювати критичність кожної прогалини в майбутніх знаннях. Наприклад, відсутність значень обов'язкових предикатів не лише знижує показник повноти, а й безпосередньо впливає на агреговану впевненість всього іменованого підграфа. Це гарантує, що навіть технічно бездоганні, але позбавлені контексту фрагментовані дані залишатимуться на динамічному рівні в статусі кандидата.

З метою уникнення впливу на описану модель знань потенційно небажаних проявів інтеграції шкідливих даних (отруєння, дезінформація, маніпуляції контекстом та семантичне спотворення) запропоновано введення багатоетапної процедури контекстної узгодженості між статичним та динамічним рівнями.

Процедура контекстної узгодженості.

Етап 1. Семантична обробка отриманих даних.

На вхід динамічного рівня надходить фрагмент напівструктурованих даних СТІ d_{in}, який визначається наступним аналітичним виразом (1):

$$d_{in} = \langle \{ \langle key_j, v_j \rangle \} \in P_{in}, r_s, p_v, t_{first}, M_{orig} \rangle, \quad (1)$$

де P_{in} – множина синтаксично коректних нормалізованих відомостей СТІ, в яких кожна пара $\langle key_j, v_j \rangle$ еквівалентна окремому предикату для S_{class} (2) – семантичної сигнатури певного класу онтології статичного рівня:

$$S_{class} = \langle N_{class}, \{ \langle key_i, w_i \rangle \} \rangle, \quad (2)$$

де N_{class} – найменування класу онтології статичного рівня; key_i – найменування предиката; w_i – ваговий коефіцієнт.

Для кожного класу онтології статичного рівня семантична сигнатура визначає набір предикатів з ваговими коефіцієнтами (обов'язкові w_i = [0,8–1,0], рекомендовані w_i = [0,6–0,8] та опціональні w_i = [0,1–0,6]), які використовуються для вибору конкретної сигнатури відносно фрагменту вхідних даних. Сукупність предикатів з найвищими ваговими коефіцієнтами ($w_i \geq 0{,}9$) формують семантичний якір v_{anchor}, на підставі якого можливо з високою ймовірністю визначити, на основі якої семантичної сигнатури на динамічному рівні необхідно створити іменований підграф G_i. Обраний набір діапазонів вагових коефіцієнтів для обов'язкових, рекомендованих та опціональних предикатів, а також порогове значення ≥ 0,9 для семантичного якоря не є визначеним у міжнародних стандартах або нормативних

документах. Однак вони узгоджується з широко розповсюдженими підходами до застосування вагових коефіцієнтів в онтологічних і семантичних системах [25; 26], а також зі стандартними конвенційними рівнями надійності у статистичних дослідженнях [27].

1.2. Ініціалізація іменованого підграфа.

Після реалізації семантичної класифікації вхідних даних відбувається генерація унікального ідентифікатора на основі найменування класу онтології статичного рівня та значень стабільних предикатів цього класу (3) [24]:

$$TYPE_{ID} = H\left(f_{can}(N_{class}) \| f_{can}(v_{anchor})\right), \tag{3}$$

де H – хеш функція; v_{anchor} – значення семантичного якоря визначеної семантичної сигнатури; f_{can} – функція канонізації, представлена виразом (4):

$$x' = f_{can}(x) = f_{lowcase}\left(f_{trim}\left(f_{clean}(x)\right)\right). \tag{4}$$

Такий підхід дає змогу уникнути міжкласових колізій шляхом створення різних просторів імен для різних сутностей, зменшити час пошуку існуючих підграфів на динамічному рівні та забезпечити незмінність ідентифікатора при інкрементальному нарощуванні фактології кандидатів у знання.

Після генерації $TYPE_{ID}$ здійснюється запит до сховища унікальних ідентифікаторів з метою виявлення еквівалентів серед існуючих кандидатів у знання на динамічному рівні. Якщо $TYPE_{ID_{in}} \ni \{TYPE_{ID_{exist}}\}$, то на динамічному рівні створюється структура, описана виразом (5):

$$G_{new} = \langle TYPE\_ID, S_{class}, V_G, P \rangle, \tag{5}$$

де V_G – множина інтегральних показників кандидата у знання, які розраховуються на момент ініціалізації, та визначаються виразом (6); P – фактологічне ядро, що складається з векторів окремих предикатів та має вигляд (7):

$$V_G = \{A_G, Conf_G, Compl_G, Cons_G, T_G\}. \tag{6}$$

$$P = \bigcup_{p \in P_{in}} \{key_p : \langle v_p, V_p, M_p \rangle\}, \tag{7}$$

де key_p – найменування предиката; v_p – значення предиката; M_p – множина метаданих походження значення цього предиката; V_p – вектор показників якості даних рівня предикатів, що має вигляд (8):

$$V_p = \langle r_s, p_v, c_p, t_{first}, t_{last}, a_p, k_p \rangle, \tag{8}$$

де оцінка впевненості в істинності факту розраховується за формулою згідно з [28]: $c_p = r_s \times p_v$, а показники a_p та k_p отримують початкові значення, що дорівнюють одиниці.

Етап 2. Збагачення іменованого підграфа та обробка семантичних конфліктів.

2.1. Підтвердження отриманих даних про кіберінцидент.

У випадку коли $TYPE_{ID_{in}} \in \{TYPE_{ID_{exist}}\}$, можливі декілька сценаріїв розвитку подій. Якщо для знайденого еквівалентного кандидата у знання значення v_p окремого предиката

key_p співпадають між собою, тоді відбувається інкрементальне підсилення існуючого факту. Для кожного предикату p значення якого збіглося, відбувається оновлення вектора V_p, а саме:

– змінюється значення інкрементального лічильника унікальних підтверджень k_p на одиницю, за умови відмінності метаданих походження фактів;

– t_{first} – залишається незмінним;

– t_{last} – оновлюється до часу надходження поточного фрагмента;

– Δt – скидається, що веде до зростання релевантності;

– оцінка впевненості в істинності значення предикату обчислюється як імовірнісна сума попереднього значення та внеску від нового джерела (9) [29]:

$$c_p = 1 - (1 - c_p, old) \times (1 - (r_{s,new} \times p_{v,new}); \quad (9)$$

– a_p – залишається незмінною ($a_p = 1$), оскільки конфлікту не виявлено.

Оновлення одного або кількох предикатів за даним сценарієм запускає ланцюгову реакцію перерахунку всього вектора V_G:

– A_G – не змінюється, оскільки семантична класифікація підтверджується і підстави сумніватись в цьому відсутні;

– $Conf_G$ – завдяки збільшенню c_p оновленого предикату загальна довіра до об'єкта підвищується;

– $Compl_G$ – не змінюється, оскільки нові значення предикатів не додавались;

– $Cons_G \to 1$ – підтвердження існуючого значення без появи альтернатив зміцнює логічну цілісність;

– T_G – темпоральна релевантність підвищується завдяки оновленню показника t_{last}.

Таким чином, після підтвердження вже існуючих фактів підграф набуває вигляду (10):

$$G_{updated} = \langle TYPE_{ID}, S_{class}, V_G(Conf_G \uparrow, T_G \uparrow), P\{key_p : \langle v_p, V_p \uparrow\rangle\}\rangle. \quad (10)$$

2.2. Збагачення іменованого підграфа новими фактами про кіберінцидент.

Якщо для знайденого еквівалентного кандидата у знання G_i структура фактологічного ядра P або значення окремих предикатів v_p відрізняються від тих, що вже зберігаються, то відбувається або розширення фасетної структури підграфа або вирішення семантичного конфлікту. Розширення відбувається через включення нового вектора предикату (11):

$$P = P_{exist} \bigcup_{p \in P_{in}} \{key_{p,new} : \langle v_{p,new}, V_{p,new}, M_{p,new}\rangle\}, \quad (11)$$

де вектор $V_{p,new}$ отримує початкові значення, аналогічно до процедури формування нового підграфа. Додавання нового значення предиката суттєво змінює V_G кандидата у знання, особливо в контексті його повноти:

– A_G – перевіряється, якщо $key_{p,new} \in S_{class}$, то A_G залишається високим, в іншому випадку знижується;

– $Conf_G$ – змінюється, якщо значення c_p для нового факту вище за середнє значення всього підграфа, то загальна довіра підвищується, в іншому випадку – знижується;

– $Compl_G$ – зростає, це головний наслідок збагачення фактології;

– $Cons_G$ – залишається стабільною через відсутність семантичних конфліктів;

– T_G – оновлюється, оскільки новий факт стає причиною підвищення релевантності всього підграфа.

Таким чином, у результаті збагачення кандидата у знання новими фактами підграф набуває вигляду (12):

$$G_{enriched} = \langle TYPE_{ID}, S_{class}, V_G(Compl_G \uparrow T_G \uparrow), P \cup \{p_{new}\}\rangle. \quad (12)$$

2.3. Обробка суперечливих даних про кіберінцидент.

Виникнення семантичного конфлікту відбувається, коли для одного й того самого предиката в межах певної семантичної сигнатури $v_{p,new} \neq v_p$. Фактологічне ядро підграфа перетворюється в множину альтернативних значень, що включає унітарні та конфліктні вектори предикатів, забезпечуючи тим самим висококонкурентне середовище та набуває вигляду (13):

$$P = \{key_p : \{\langle v_{p1}, V_{p1}, M_{p1}\rangle, \langle v_{p2}, V_{p2}, M_{p2}\rangle, \dots, \langle v_{pn}, V_{pn}, M_{pn}\rangle\}\}. \quad (13)$$

Для кожного значення предиката v_{pn} розраховуються та встановлюються початкові значення показників якості даних V_{pn}, а також для всіх альтернатив key_p оновлюється значення a_p до числа, що дорівнює кількості альтернатив. Семантичний конфлікт суттєво знижує значення показника готовності, оскільки знижуються значення основних показників рівня підграфа $Cons_G$ та A_G, які безпосередньо впливають на узгодженість кандидата у знання G_i з наявною моделлю знань. Наявність суперечливих значень ключових предикатів ставить під сумнів точність семантичної класифікації S_{class} та суттєво знижує агреговану впевненість всього підграфа. Таким чином, після надходження альтернативних значень предикатів, що викликало виникнення локального семантичного конфлікту підграф має наступний вигляд (14):

$$G_{conflict} = \langle TYPE_{ID}, S_{class}, V_G(Cons_G \downarrow, A_G \downarrow), P\{key_p : \{\langle v_{p1}, V_{p1}, M_{p1}\rangle, \langle v_{p2}, V_{p2}, M_{p2}\rangle, \dots, \langle v_{pn}, V_{pn}, M_{pn}\rangle\}\}\rangle. \quad (14)$$

У цьому випадку виникнення навіть одного локального конфлікту унеможливлює перехід кандидата G_i на рівень знань. Реалізація сценарію 2.1 відносно одного з конкуруючих значень предиката іменованого підграфа G_i сприятиме підвищенню показників якості даних рівня предикатів V_p та призведе до його остаточного домінування над іншими значеннями та перерахунку показників якості даних всього вектора V_G. У випадку перебування кандидата G_i на динамічному рівні протягом тривалого часу передбачається реалізація підходу "Людина в циклі" [30], коли експерт оцінює контекст конфліктної ситуації та приймає рішення щодо її усунення.

Етап 3. Прийняття рішення про підвищення кандидата G_i до рівня знання.

3.1. Оцінка готовності даних до набуття статусу формалізованих знань.

Процедура контекстної узгодженості отриманих вхідних даних з домену кіберзахисту з існуючою моделлю знань визначається як нелінійний ітеративний алгоритм обробки вхідних даних, покликаний оцінити ступінь семантичного резонансу на вході динамічного рівня, знизити рівень ентропії кандидатів у знання та ініціювати процедуру їх формалізації як повноцінних екземплярів відповідних класів онтології на підставі обчислення агрегованого показника готовності R_G (15):

$$R_G = (A_G \times Cons_G) \times (\alpha Compl_G + \beta Conf_G + \gamma T_G). \quad (15)$$

Оскільки не існує універсальних коефіцієнтів важливості показників якості даних, ваги α, β, γ у запропонованій моделі вводяться як контекстно-залежні коефіцієнти, що відображають вплив відповідних показників на прийняття рішень у конкретній ситуації. У цьому випадку $\alpha = 0{,}2, \beta = 0{,}5, \gamma = 0{,}3$, у зв'язку з тим, що сумнівне походження ідеально наповнених фрагментів даних може свідчити про факт дезінформації або наміру отруєння моделі, що не надає достатньої інформаційної цінності.

Для оцінки релевантності кіберрозвідданих T_G найбільш доцільним є сигмоїдальне згасання, оскільки для більшості загроз вони залишаються критично важливими протягом обмеженого проміжку часу, після чого їхня цінність стрімко падає, коли ІСК адаптуються під кібератаку або зловмисники змінюють її вектор [11]. Це дослідження показує, що широко вживана експоненціальна крива Еббінгауза часто поступається сигмоїдальній та інверсній функціям у моделюванні реальних процесів втрати актуальності. Розрахунок темпоральної релевантності на основі сигмоїдального згасання з урахуванням хронологічних метаданих рівня предикатів зводиться до наступного аналітичного виразу (16) [11]:

$$T_G = \frac{1}{1 + e^{-k(\min(\Delta t) - \tau)}}, \tag{16}$$

де $\Delta t = t_{now} - t_{last}$ – час з моменту останнього оновлення значення предикату; τ – горизонт актуальності спостереження, визначає момент коли актуальність починає різко спадати; k – коефіцієнт крутизни спаду, визначає, наскільки швидко факт втрачає релевантність за межами горизонту актуальності спостереження.

Розрахунок агрегованої впевненості $Conf_G$ здійснюється відносно наявної фактології без врахування відсутніх значень предикатів семантичної сигнатури (17) [31]:

$$Conf_G = \frac{\sum\left(\frac{\max(c_{pi})}{a_{pi}} \times w_i\right)}{\sum w_i}. \tag{17}$$

Структурна повнота $Compl_G$ відображає ступінь наповнення іменованого підграфа G_i доступною фактологією відносно еталонного набору даних, передбаченого семантичною сигнатурою S_{class} (18) [32]:

$$Compl_G = \frac{\sum n_{filled}}{\sum n_{ss}}, \tag{18}$$

де n_{filled} – кількість заповнених значеннями предикатів іменованого підграфа G_i; n_{ss} – кількість предикатів, які передбачені семантичною сигнатурою S_{class}.

Наявність суперечливих значень у ключових полях ставить під сумнів точність семантичної класифікації S_{class}, тому розрахунок значення загального показника узгодженості $Cons_G$ здійснюється з урахуванням показників кардинальності доступних значень предикатів іменованого підграфа (19) [33]:

$$Cons_G = \frac{n_{ss}}{n_{filled}} \times \sum_{i=1}^{n_{filled}} \frac{1}{a_{pi}}. \tag{19}$$

Точність семантичної класифікації A_G відіграє важливу роль у розрахунку загального показника готовності R_G, оскільки саме від неї залежить наскільки високими будуть показники

повноти, впевненості та узгодженості. Логіка розрахунку ґрунтується на принципі ймовірнісного об'єднання незалежних свідчень, що є апроксимацією часткового випадку теорії Демпстера – Шафера [34], та має вигляд (20):

$$A_G = 1 - \prod_{i \in v_{anchor}} (1 - w_i). \tag{20}$$

Таким чином, узгоджені свідчення взаємно підсилюють одне одного, тоді як суперечливі зменшують точність класифікації через нормалізацію, що забезпечує інтуїтивно коректне агрегування незалежних джерел інформації в умовах неповноти та конфліктності даних.

Кожного разу, коли до іменованого підграфа G_i на динамічному рівні застосовується один із сценаріїв підтвердження або розширення наявної фактології, вирішення семантичних конфліктів, агрегований показник його готовності R_G до набуття статусу формалізованих знань перераховується та порівнюється із пороговим значенням. Позитивний результат порівняння ініціює процес формалізації фактологічного ядра P кандидата у знання G_i у відповідний набір RDF-триплетів (базова одиниця представлення знань у моделі Resource Description Framework) екземпляра відповідного класу онтології статичного рівня, що інтерпретується як перехід між її поточним та потенційно більш контекстуально насиченим станами. Формально модель організації знань описується наступним аналітичним виразом (21):

$$L_{stat}(j+1) = L_{stat}(j) \cup \{G_i \in L_{dyn}(j) : R_G(G_i) \geq \theta\}, \tag{21}$$

де L_{stat} – множина формалізованих знань до моменту набуття кандидатом у знання значення показника готовності $\theta_{min} \geq 0{,}7$; L_{dyn} – множина кандидатів у формалізовані знання; G_j – іменований підграф, що репрезентує сукупність відомостей про кіберінцидент.

Враховуючи відсутність у міжнародних стандартах фіксованих числових значень порогів щодо якості даних, зокрема в [20], у яких значення визначаються контекстно як мінімальний рівень, достатній для практичного використання знань у процесах прийняття рішень. Порогове значення $\theta_{min} = 0{,}7$ обрано як емпіричний компроміс між вимогами до релевантності, впевненості, логічної узгодженості та повноти знань та відповідає загальноприйнятій практиці в інтелектуальному аналізі даних, де рівень 0,7 інтерпретується як межа переходу від слабких до операційно придатних оцінок знань [27].

Для забезпечення перевірки того, чи зберігається логічна узгодженість під час масштабування онтології статичного рівня передбачається поєднання двох механізмів онтологічного виведення (HermiT та Pellet) [35; 36]. Завдяки оптимізації детермінованих кроків виведення HermiT надає можливість перевірки цілісності всієї онтології, забезпечуючи виявлення порушення функціональних властивостей або циклічних визначень. Однак продуктивність HermiT має свою ціну, механізми інтерпретації виявлених розбіжностей часто менш деталізовані, що може ускладнити діагностику при інтеграції нових знань. Тому для вирішення виявлених конфліктів на локальному рівні передбачено застосування логічного висновувача Pellet, який безпосередньо вказує на конкретну множину аксіом, що призвели до нього, що призводить до зменшення часу обробки семантичних колізій. Таким чином, перевірка нового стану моделі знань $L_{stat}(j+1)$ реалізується як дворівневий процес, у якому HermiT та *Pellet* підтверджують логічну узгодженість, розраховану на основі (19).

Результати дослідження

Для оцінки ефективності запропонованої моделі було обрано набори даних [37–40]. Онтологічну основу для накопичення формалізованих знань реалізовано відповідно до концептуальної схеми, зазначеної на рисунку 2.

Критерії оцінки ефективності запропонованої моделі включали середні значення показників готовності R_G, узгодженості $Cons_G$, повноти $Compl_G$, агрегованої впевненості $Conf_G$ та темпоральної релевантності T_G для іменованих підграфів $\{G_1, G_2, \dots, G_n\}$, які були обрані для подальшої формалізації як екземпляри відповідних класів.

Суть експерименту полягала у реалізації контрольованої інтеграції динамічних потоків фрагментованих даних з [37–40] через процедуру контекстної узгодженості між динамічним і статичним рівнями на основі розрахунку комплексного показника готовності R_G кандидатів у знання G_i з подальшим визначенням ступеня впливу потенційного елемента моделі знань на здатність онтології підтримувати формування логічних висновків в межах поточного контексту.

Результати проведеного експерименту:

- загальна кількість ітерацій процедури контекстної узгодженості – 36 824;
- загальна кількість ініційованих сценарії підтвердження наявної фактології – 1 985;
- загальна кількість ініційованих сценарії розширення наявної фактології – 1 693;
- загальна кількість локальних конфліктів – 436;
- загальна кількість доданих до онтології нових сутностей – 23 830;
- загальна кількість кандидатів у формалізовані знання, які залишились у просторі динамічного рівня – 8 880;
- середнє значення показника готовності доданих до онтології нових сутностей – 0,76;
- середнє значення показника повноти доданих до онтології нових сутностей – 0,32;
- середнє значення показника впевненості доданих до онтології нових сутностей – 0,82;
- середнє значення показника узгодженості доданих до онтології нових сутностей – 0,99;
- середнє значення показника релевантності доданих до онтології нових сутностей – 0,99.

Варто зазначити, що перевірка логічної узгодженості онтології в результаті істотного збагачення її фактологічного змісту під час експерименту (засобами HermiT) показала відсутність порушень функціональних властивостей та циклічних визначень, тоді як засобами Pallet було виявлено незначну кількість локальних конфліктів. Аналіз діагностичних даних про виявлені конфлікти показав, що вони виникли внаслідок розбіжності у термінології опису певних аспектів кіберінцидентів у наборах MITRE та EuRepoC. Враховуючи ступінь гетерогенності вхідних даних, запропонована модель демонструє достатньо високий показник ефективності відбору кандидатів у формалізовані знання, що свідчить про її значний потенціал для сучасних ІСК.

На рисунку 3 представлено побудовану онтологію кіберзагроз після збагачення її фактологічного змісту у вигляді графа. З метою уникнення візуальної надмірності кількість екземплярів відповідних класів суттєво обмежена.

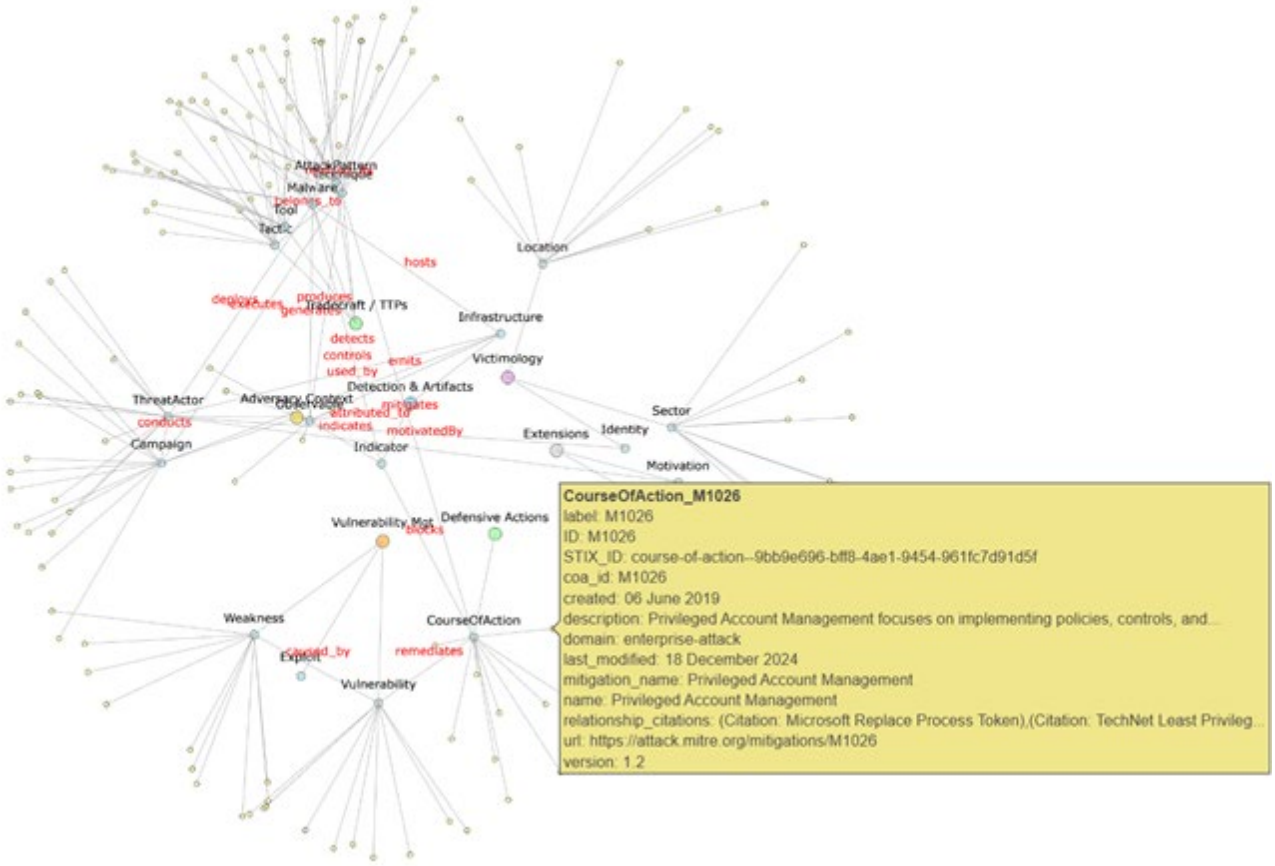

Рис. 3. Онтологія кіберзагроз після збагачення її фактологічного змісту у вигляді графа

Висновки та перспективи подальших досліджень. У статті запропоновано модель дворівневої організації знань в ІСК на онтологічній основі. На відміну від існуючих підходів, які переважно зосереджені на поверхневій консолідації онтологічних ресурсів окремих постачальників, запропонований підхід спрямований на формалізацію процесу контрольованої інтеграції динамічних потоків фрагментованих даних з домену кіберзахисту через процедуру контекстної узгодженості між динамічним і статичним рівнями на основі розрахунку комплексного показника готовності кандидатів у знання. Розроблено федеративну онтологію, структура якої узгоджується з підходами побудови кібербезпекових графів знань, у яких сутності та їхні відношення описані відповідно до функціональних аспектів домену. Реалізовано процедуру контекстної узгодженості як нелінійний ітеративний алгоритм обробки вхідних даних, покликаний оцінити ступінь семантичного резонансу на вході динамічного рівня, знизити рівень ентропії кандидатів у знання та ініціювати процедуру їх формалізації як повноцінних екземплярів відповідних класів онтології.

Результати дослідження показали, що незважаючи на істотне збагачення фактологічного змісту 23 830 новими сутностями з середнім показником їх готовності 0,76, показник узгодженості онтології залишився на рівні 99 %, з урахуванням виникнення незначної кількості локальних конфліктів. Отримані результати свідчать про ефективність запропонованого підходу щодо забезпечення семантичної та концептуальної цілісності онтології при безперервному надходженні гетерогенних даних кіберрозвідки з урахуванням вимог до їхньої якості та достовірності у процесі інтеграції.

Перспективним напрямком подальших досліджень є розробка моделі контекстно-орієнтованої інтеграції знань з елементами самонавчання.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Refereed Proceedings Papers. KM Conference 2025 (Knowledge Management, Cybersecurity, Learning, Information Technology). Siena, Italy, 2025. URL: https://www.iiakm.org/conference/proceedings/KM2025_RefereedProceedingsPapers.pdf.

2. Фесьоха В. В., Легкобит В. С., Чернявський Р. Г., Романенко С. О. Аналіз підходів до реалізації життєвого циклу управління знаннями в інтелектуальних системах кіберзахисту // Вісник Вінницького політехнічного інституту. 2025. № 4 (181). С. 95–107. URL: https://doi.org/10.31649/1997-9266-2025-181-4-95-107.

3. Syed Z., Padia A., Mathews M. L., Finin T., Joshi A. UCO: A Unified Cybersecurity Ontology. Proceedings of the AAAI Workshop on Artificial Intelligence for Cyber Security. 2016. URL: https://ebiquity.umbc.edu/_file_directory_/papers/781.pdf.

4. Oltramari A., Cranor L. F., Walls R. J., McDaniel P. Building an ontology of cyber security // CEUR Workshop Proceedings. 2014. № 1304. P. 54–61. URL: https://ceur-ws.org/Vol-1304/STIDS2014_T08_OltramariEtAl.pdf.

5. Christian R., Dutta S., Park Y., Rastogi N. An Ontology-driven Knowledge Graph for Android Malware. Proceedings of the ACM SIGSAC Conference on Computer and Communications Security. 2021. P. 2435–2437. URL: https://doi.org/10.1145/3460120.3485353.

6. Akbar A., Rahman F., Singhal A., Khan L., Thuriasingham B. The Design and Application of a Unified Ontology for Cyber Security. Information Systems Security. 2023. P. 1–15. URL: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=956387.

7. Obrst L., Chase P., Markeloff R. Developing an Ontology of the Cyber Security Domain // CEUR Workshop Proceedings. 2012. № 966. P. 49–56. URL: https://ceur-ws.org/Vol-966/STIDS2012_T06_ObrstEtAl_CyberOntology.pdf.

8. Zhou J., Song X., Li Y., Gao Y., Zhang X. Building Real-Time Ontology Based on Adaptive Filter for Multi-Domain Knowledge Organization // IEEE Access. 2021. № 9. P. 66486–66497. URL: https://doi.org/10.1109/ACCESS.2021.3076833.

9. Satyapanich T., Ferraro F., Finin T. CASIE: Extracting Cybersecurity Event Information from Text. Proceedings of the AAAI Conference on Artificial Intelligence. 2020. № 34 (5). С. 8749–8757. URL: https://doi.org/10.1609/aaai.v34i05.6401.

10. Giunchiglia F., Bagchi M., Das S. From Knowledge Organization to Knowledge Representation and Back. 2024. URL: https://doi.org/10.48550/arXiv.2401.11753.

11. Sha A., Gu Z., Nunes B.P., Gu Z. Is there a better way to forget? Modelling memory decay in deep knowledge tracing. Knowledge-Based Systems. 2026. Vol. 332. P. 114884. URL: https://doi.org/10.1016/j.knosys.2025.114884.

12. Valero‑Jorquera J. M., López Martínez A., Sánchez‑Sánchez P.M., Navarro‑Martínez D. Unlocking the Potential of Knowledge Graphs: A Cyber Defense Ontology for a Knowledge Representation and Reasoning System // Proceedings of the ACM Web Conference (WWW) / The Web Conf. 2024. URL: https://doi.org/10.1145/3664476.3670916.

13. Jin B., Kim E., Lee H., Bertino E., Kim D., Kim H. Sharing cyber threat intelligence: Does it really help? Proceedings of the 31st Network and Distributed System Security Symposium (NDSS 2024), San Diego, CA, USA, 2024. URL: https://doi.org/10.14722/ndss.2024.24228.

14. Gu Z., Lanti D., Corcoglioniti F., Montali M., Poggi A., Maccani M., Calvanese D., Xiao G. Ontology‑based data federation and query optimization // Knowledge‑Based Systems. 2025. Vol. 329 (Part A). P. 1–26. URL: https://doi.org/10.1016/j.knosys.2025.114216.

15. Wimmer H., Yoon V., Rada R. Applying Semantic Web Technologies to Ontology Alignment // International Journal of Intelligent Information Technologies. 2012. Vol. 8, no. 1. P. 1–9. URL: https://doi.org/10.4018/JIIT.2012010101.

16. Codescu M., Kuksa E., Kutz O., Mossakowski T., Neuhaus F. Ontohub: A semantic repository for heterogeneous ontologies. 2016. URL: https://doi.org/10.48550/arXiv.1612.05028.

17. OODA Loops // Iterum. URL: https://iterum.co.uk/ooda-loops.

18. Staves A., Gouglidis A., Hutchison D. An Analysis of Adversary‑Centric Security Testing within Information and Operational Technology Environments // Digital Threats: Research and Practice. 2023. Vol. 4, no. 1. Article 14. P. 1–29. URL: https://doi.org/10.1145/3569958.

19. Sikos L. F. Cybersecurity knowledge graphs // Knowledge and Information Systems. 2023. Vol. 65, no. 3. P. 3511–3531. URL: https://doi.org/10.1007/s10115-023-01860-3.

20. ISO/IEC 25012: Data Quality model // ISO/IEC 25000 Standards Portal. URL: https://iso25000.com/index.php/en/iso-25000-standards/iso-25012.

21. DAMA‑DMBOK®2 Revised Edition – FAQs // DAMA International. URL: https://dama.org/dama-dmbok2-revised-edition-faqs.

22. W3C Data Quality Vocabulary (DQV). Web Content – Data on the Web Best Practices: Data Quality Vocabulary // World Wide Web Consortium (W3C), 2016. URL: https://www.w3.org/TR/vocab-dqv.

23. NIST Cybersecurity Framework (CSF) // National Institute of Standards and Technology (NIST). URL: https://www.nist.gov/cyberframework.

24. The CBOR, dCBOR, and Gordian Envelope Book: Introduction. URL: https://cborbook.com/introduction/cover.html.

25. Atencia M., Borgida A., Euzenat J., Ghidini C., Serafini L. A Formal Semantics for Weighted Ontology Mappings. The Semantic Web – ISWC 2012 // Lecture Notes in Computer Science. 2012. № 7649. P. 17–33. URL: https://disi.unitn.it/~p2p/RelatedWork/Matching/atencia2012c.pdf.

26. Keikha M. M., Nematbakhsh M. A., Tork Ladani B. Structural Weights in Ontology Matching // International Journal of Web & Semantic Technology (IJWesT). 2013. № 4. P. 41–58. URL: https://doi.org/10.48550/arXiv.1311.3800.

27. Izah S.C., Sylva L., Hait M. Cronbach's Alpha: A Cornerstone in Ensuring Reliability and Validity in Environmental Health Assessment // ES Energy & Environment. 2023. Vol. 23. Article 1057. URL: https://dx.doi.org/10.30919/esee1057.

28. JDP 2‑00 (4th Edition): Intelligence, Counter‑intelligence and Security Support to Joint Operations. United Kingdom Ministry of Defence (MOD). 2023. URL: https://assets.publishing.service.gov.uk/media/653a4b0780884d0013f71bb0/JDP_2_00_Ed_4_web.pdf.

29. Csenki A. Independent events in elementary probability theory // International Journal of Mathematical Education in Science and Technology. 2011. № 42 (6). P. 685–691. URL: https://doi.org/10.1080/0020739X.2011.562313.

30. Keet C. M., Grütter R. Toward a systematic conflict resolution framework for ontologies // Journal of Biomedical Semantics. 2021. № 12 (1). P. 15. URL: https://doi.org/10.1186/s13326-021-00246-0.

31. Tchakounté F., Faissal A., Atemkeng M., Ntyam A. A Reliable Weighting Scheme for the Aggregation of Crowd Intelligence to Detect Fake News // Information. 2020. № 11 (6). P. 319. URL: https://doi.org/10.3390/info11060319.

32. Ehrlinger L., Wöß W. A Survey of Data Quality Measurement and Monitoring Tools // Frontiers in Big Data. 2022. № 5. P. 850611. URL: https://doi.org/10.3389/fdata.2022.850611.

33. Bisewski K., Hashorva E., Shevchenko G. The harmonic mean formula for random processes // International Journal of Computer Mathematics. 2022. № 99 (4). P. 591–603. URL: https://doi.org/10.1080/07362994.2022.2055574.

34. Mercier D., Lefevre E. Introduction to Dempster-Shafer Theory of Belief Functions // Tutorial PFIA 2022. 2022. URL: https://davidmercier.fr/talks/2022_PFIA_BFintro.pdf.

35. Glimm B., Horrocks I., Motik B., Stoilos G., Wang Z. HermiT: An OWL 2 Reasoner // Journal of Automated Reasoning. 2014. Vol. 53. P. 245–269. URL: https://doi.org/10.1007/s10817-014-9305-1.

36. Sirin E., Parsia B., Cuenca Grau B., Kalyanpur A., Katz Y. Pellet: A practical OWL-DL reasoner // Journal of Web Semantics. 2007. № 5 (2). P. 51–53. URL: https://doi.org/10.1016/j.websem.2007.03.004.

37. MITRE. Enterprise ATT&CK Framework. Версія 18.1. 2026. URL: https://attack.mitre.org/docs/attack-excel-files/v18.1/enterprise-attack/enterprise-attack-v18.1.xlsx.

38. MITRE. Common Attack Pattern Enumeration and Classification (CAPEC). Версія 3.9. 2026. URL: https://capec.mitre.org/data/archive/capec_v3.9.zip.

39. EuRepoC. Global Dataset of Cyber Incidents. Версія 1.3.2. 2025. URL: https://doi.org/10.5281/zenodo.14965395.

40. EuRepoC. Global Dataset of Cyber Incidents. Версія 1.2. 2024. URL: https://doi.org/10.5281/zenodo.11108195.

Надійшла до редколегії 07.04.2026.
Схвалена до друку 22.05.2026.
Дата публікації 29.05.2026.