https://doi.org/10.31649/1997-9266-2025-181-4-95-107

УДК 004.853

В. В. Фесьоха[1]
В. С. Легкобит[1]
Р. Г. Чернявський[2]
С. О. Романенко[1]

АНАЛІЗ ПІДХОДІВ ДО РЕАЛІЗАЦІЇ ЖИТТЄВОГО ЦИКЛУ УПРАВЛІННЯ ЗНАННЯМИ В ІНТЕЛЕКТУАЛЬНИХ СИСТЕМАХ КІБЕРЗАХИСТУ

[1] Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ;
[2] Центральний науково-дослідний інститут Збройних Сил України, Київ

Досліджено завдання ефективного управління знаннями в інтелектуальних системах кіберзахисту з метою підвищення їх здатності виявляти, інтерпретувати та попереджати сучасні кіберзагрози. Обґрунтовано, що досягнення високого рівня їх адаптивності та ситуаційної обізнаності можливе лише за умови реалізації повного життєвого циклу управління знаннями, який охоплює етапи здобування, інтеграції, організації, застосування та оновлення.

Здійснено порівняльний аналіз сучасних підходів до реалізації ключових фаз управління знаннями в інтелектуальних системах кіберзахисту. Особливу увагу приділено аналізу підходів до організації знань, таких як онтологічне моделювання, графи знань, продукційні правила, фрейми, нейромережеві структури та семантичні мережі. Розглянуто відповідні мови подання знань, протоколи обміну інформацією про загрози, а також інструменти для добування знань. Отримані результати свідчать, що жоден з розглянутих підходів не забезпечує повної відповідності визначеним критеріям ефективного управління знаннями, зокрема структурованості, актуальності, інтерпретованості, масштабованості, гнучкості, обчислювальної ефективності та прозорості прийняття рішень. У зв'язку з цим обґрунтовано доцільність створення гібридної архітектури управління знаннями, яка поєднує переваги різних підходів.

Запропоновано функціональну схему, яка інтегрує онтологічне ядро з модулями самонавчання, автоматичної генерації правил, верифікації та зворотного зв'язку. Представлений підхід забезпечує наскрізну обробку знань від видобутку до практичного застосування у вигляді обґрунтованих рішень у реальному часі. Це створює підґрунтя для побудови інтелектуальних систем кіберзахисту нового покоління, здатних до самовдосконалення та стійкого реагування на загрози в умовах динамічного кіберсередовища.

Ключові слова: управління знаннями, інтелектуальні системи кіберзахисту, штучний інтелект, інформаційно-комунікаційні системи, кіберзагрози, кіберстійкість.

Вступ

Наразі завдання протистояння складності, що зростає, та непередбачуваності кібератак на ключові інформаційно-комунікаційні системи (ІКС) покладено на інтелектуальні системи кіберзахисту (ІСК) — програмні або програмно-апаратні рішення (Security Information and Event Management (SIEM), User and Entity Behavior Analytics (UEBA), Endpoint/Extended Detection and Response (EDR/XDR), Network Detection and Response (NDR), Security Orchestration, Automation and Response (SOAR)), що інтегрують модулі збору, аналізу, кореляції та інтерпретації подій безпеки в режимі реального часу з використанням алгоритмів штучного інтелекту (ШІ), машинного навчання, методів ситуаційного моделювання та управління знаннями.

Ключовою особливістю таких систем є можливість не лише реєструвати та реагувати на кіберінциденти, а й прогнозувати потенційні загрози, виявляти приховані об'єктивні закономірності, узагальнювати попередній досвід, формувати адаптивні сценарії протидії та автоматично оновлювати захисні політики відповідно до змін середовища. Зазвичай, це досягається завдяки їхній здат-

ності навчатися (донавчатися) на релевантних даних щодо технік (стратегій) реалізації та/або ознак кібератак [1].

Відтак, ефективність функціонування ІСК визначається якістю процесу управління знаннями, що включає своєчасне оновлення, повноту та коректну інтерпретацію інформації про кіберзагрози, її інтеграцію до системи кіберзахисту, організацію, упорядкування, необхідних для навчання та прийняття обґрунтованих рішень в процесі забезпечення кіберстійкості ІКС [2].

Проте, незважаючи на значну кількість наукових праць, щодо розробки підходів до управління знаннями в ІСК, завдання їх ефективного застосування в умовах безперервної еволюції загроз залишається актуальним, що підтверджується численними кіберінцидентами, спричиненими недостатньою актуальністю даних про кібератаки [3]—[6].

Зазначене зумовлює доцільність подальших наукових досліджень щодо підвищення ефективності застосування ІСК на основі розробки нових методів управління знаннями.

Аналіз попередніх досліджень та публікацій

Аналіз попередніх досліджень та публікацій [7]—[22] демонструє значні досягнення в розробці (удосконаленні) моделей та методів управління знаннями для потреб кібербезпеки за кількома напрямами. Так, у низці досліджень розглядається потенціал управління знаннями для посилення спроможностей ІСК шляхом використання онтологій, графів знань, моделей на основі правил та технологій ШІ, що дає змогу формалізовано представляти, інтегрувати та оновлювати знання про кібератаки, вразливості та захисні механізми [7]—[11], [12], [14]. Ці підходи досить ефективно поєднують інформацію з гетерогенних джерел, підвищуючи ситуаційну обізнаність і підтримуючи логічний висновок у складних сценаріях. Разом з тим, залишається недостатня інтероперабельність форматів даних, а також потреба в стандартизації механізмів оновлення знань.

Окремі роботи зосереджені на розробці ІСК, які поєднують онтології з методами машинного навчання, обробки природної мови, логічного виводу, правил та передавального навчання, що дає змогу досягти високої точності, швидкого оновлення знань та адаптації до нових кіберзагроз [10]—[13], [15]. Проте зазначені підходи залишаються обмеженими в протидії кібератакам нульового дня, містять складності інтерпретації природної мови, а також логічних конфліктів у разі оновлення знань.

Суттєвий внесок у розвиток адаптивного управління знаннями в ІСК здійснюють гібридні системи, які поєднують логіко-семантичне моделювання, нечітку логіку, глибоке навчання та когнітивне моделювання [13]—[20]. Результати досліджень демонструють високу ефективність у виявленні аномалій, аналізі зашифрованого трафіку, генерації правил та візуалізації загроз, де особливо виділяються спайкові нейронні мережі, архітектура Lambda, AutoML-рішення та методи CTI-mining, здатні до самонавчання. Разом з цим, спостерігаються обмеження у прозорості рішень, втраті інформації під час попередньої обробки, а також потреба в значних обчислювальних ресурсах.

Інший напрям досліджень зосереджений на формуванні інтегрованих моделей управління знаннями на основі міжнародних стандартів (ISO/IEC 15408, ISO/IEC 18045), а також з урахуванням організаційних, технологічних, людських і процесних факторів [15], [19]—[22], зокрема враховано роль краудсорсингу, когнітивних та культурних чинників, ситуаційної обізнаності, Zero Trust-архітектури та візуалізації загроз. Проте залишаються відкритими питання якісної інтеграції неструктурованих знань, ручної валідації, стандартизації даних і узгодженості моделей.

Таким чином, основними науковими викликами в управлінні знаннями для ІСК залишаються: забезпечення оперативного оновлення знань, подолання семантичного бар'єра між джерелами даних про кіберзагрози, інтероперабельність форматів даних, а також прозорість прийняття рішень в процесі виявлення кібератак.

У зв'язку з цим, *метою статті* є проведення порівняльного аналізу підходів до реалізації життєвого циклу управління знаннями в ІСК та визначення перспективних напрямів усунення зазначених недоліків.

Основна частина дослідження

Управління знаннями в ІСК — це багатоаспектний циклічний процес, який охоплює повний життєвий цикл роботи з інформацією про кіберзагрози, вразливості та способи протидії. Цей процес забезпечує здатність системи пропонувати обґрунтовані рішення на основі отриманого (набутого) досвіду, а також сприяє підвищенню її адаптивності, узгодженості, ситуаційної обізнаності

та ефективності в умовах динамічних змін у кіберпросторі. В сучасній науковій та прикладній літературі описано низку загальновизнаних моделей життєвого циклу управління знаннями, серед яких Wiig-Model, Meyer & Zack, Bukowitz & Williams, McElroy, Dalkir's Integrated KM Cycle, а також фреймворк APQC і стандарт ISO 30401 [23]—[25]. Попри варіативність термінології та деталізацію зазначені моделі описують подібні життєві цикли, які можна узагальнити до спільних фаз управління знаннями в ІСК: видобуток, інтеграція, організація, зберігання, застосування та оновлення знань, які показано на рис. 1.

Очевидно, ефективне управління знаннями в ІСК вимагає не лише вдосконалення окремих процесів, а й забезпечення узгодженої взаємодії всіх фаз життєвого циклу. Оскільки кожна з них виконує критично важливу функцію щодо забезпечення здатності системи своєчасно реагувати на нові загрози, адаптуватися до змін у середовищі та підтримувати ситуаційну обізнаність, доцільним є не загальний огляд підходів до управління знаннями, а саме поетапний аналіз наявних підходів до реалізації кожної з фаз життєвого циклу. До того ж, вищезгадані моделі управління знаннями хоч і формують важливу методологічну основу для розуміння структури процесу, залишаються надто загальними для практичної реалізації в умовах функціонування ІСК.

Рис. 1. Узагальнені фази життєвого циклу управління знаннями в ІСК

У статті основна увага зосереджена на тих фазах управління знаннями, які є методологічно складними та критичними для ефективного функціонування ІСК: **застосування**, **організації**, **інтеграції** та **видобутку** знань. Інші фази життєвого циклу, зокрема **зберігання** та **оновлення** знань є також важливими, однак їх реалізація в ІСК є більш прикладною та менш проблемною з погляду теоретичного обґрунтування.

Серед зазначених фаз управління знаннями особливе значення для оперативного функціонування ІСК має **застосування знань**, адже саме на цьому етапі накопичений інтелектуальний ресурс перетворюється на інструмент прийняття рішень, трансформуючи пасивні знання у конкретні дії або зміни станів системи. Порівняльний аналіз підходів до реалізації застосування знань в ІСК подано в табл. 1.

Таблиця 1

Порівняльний аналіз підходів до реалізації застосування знань в ІСК

Підхід до застосування знань	Особливості	Переваги	Недоліки
Генерація правил	Фіксовані правила та бази знань. Дедуктивні, асоціативні методи формування висновків	Висока інтерпретованість та швидкість спрацьовування врахування невизначеності, неповноти — нечіткі правила, правила на основі довіри	Потребують ручного оновлення, складність масштабування
Машинне навчання	data mining, статистичні методи формування висновків	Швидкість обробки великих обсягів даних, масштабованість, динамічна адаптація	Складність інтерпретації, потреба у верифікації
Семантичне і онтологічне виведення	Структуроване зберігання знань, семантичні методи формування висновків	Виявлення глибоких закономірностей, високий рівень формалізації	Високі накладні витрати при інтенсивному масштабуванні
Візуальна аналітика	Застосування графів знань, теплових та когнітивних мап	Прискорене розуміння ситуації	Висока залежність від якості вихідних даних
Формування гіпотез	Використання інфраструктурних метаданих (топології, симуляції, часові вікна) контекстуальні методи формування висновків	Фокусує увагу аналітиків на найвірогідніших сценаріях, сприяє генеруванню нетривіальних припущень	Необхідність механізмів пріоритизації й ризико-орієнтованого ранжування, потреба додаткової інфраструктури тестування сценаріїв

В сучасних ІСК описані підходи здебільшого використовуються у поєднанні, залежно від цілей системи та джерел знань:

– ***генерація правил*** передбачає формування кореляційних механізмів за допомогою алгоритмів дедуктивного та асоціативного виведення (Apriori, FP-growth) та застосовується переважно в SIEM, IDS/IPS, SOAR;

– застосування знань в ***машинному навчанні*** характеризується їх відображенням в параметрах моделей для класифікації аномалій, прогнозування кіберзагроз та побудови поведінкових профілів (UEBA, EDR/XDR);

– ***семантичне та онтологічне виведення*** все частіше використовується в системах управління знаннями для кіберзахисту, особливо для інтеграції різнорідних джерел (наприклад, STIX/TAXII, MITRE ATT&CK);

– інструменти для ***візуалізації*** в свою чергу перетворюють багатовимірні знання на інтерактивні дашборди для підтримки когнітивного аналізу ситуацій (Maltego, Kibana);

– ***гіпотетичні сценарії*** кібератак, що генеруються на основі комбінованих знань за допомогою великих мовних моделей, часто формують підґрунтя для реалізації проактивних стратегій захисту.

Проведений аналіз і результати досліджень [26]— [28] провідних компаній світу доводять ефективність застосування комбінованих підходів, наприклад, IBM QRadar, Elastic SIEM, Microsoft Sentinel часто поєднують генерацію правил з аналітикою на основі машинного навчання, Palo Alto Cortex XSOAR, IBM Resilient, Splunk Phantom використовують формалізовані протоколи реагування на події в системі, Microsoft Defender XDR, CrowdStrike Falcon, Palo Alto Cortex XDR застосовують алгоритми ШІ для кореляційного аналізу складних кіберзагроз на підставі зібраної телеметрії з кінцевих точок.

З інноваційним підходом до підвищення кіберстійкості ІКС [29], знання, які накопичуються та використовуються в ІСК, мають бути не лише актуальними, а й зрозумілими для сприйняття людиною (принцип інтерпретованості/обізнаності). Досягнення необхідного балансу між своєчасним оновленням знань та прозорістю наданих рекомендацій та (або) прийнятих рішень значною мірою визначається формою організації знань в системі. У зв'язку з цим, порівняльний аналіз підходів до **організації знань** в ІСК доцільно здійснювати за такими критеріями [30], [31]: *структурованість, актуалізація, інтерпретованість, нормалізація, стабільність*.

Рис. 2. Результати порівняльного аналізу підходів до організації знань в ІСК

На рис. 2 показано результати порівняльного аналізу онтологічного, фреймового, нейромережевого, семантично мережевого та заснованого на правилах підходів до організації знань в ІСК за описаними критеріями, що відображає рівень відповідності кожного підходу у відсотках.

Онтологічний [30] підхід забезпечує системне представлення предметної області, що об'єднує два важливі аспекти: формальну семантику знань для автоматизованої обробки за допомогою алгоритмів машинного навчання та семантику реального світу для розуміння людиною. Завдяки використанню чітко визначених понять, властивостей і відношень, онтології демонструють найвищий рівень *структурованості* (≈95 %) серед усіх розглянутих підходів. Застосування принципів когерентної термінології, аксіоматизації та технологій Semantic Web забезпечує високий рівень *нормалізації* знань (≈90 %), що дозволяє узгоджувати гетерогенні джерела, інтегрувати множинні онтології та уникати термінологічних конфліктів. Онтології є *стабільною* основою для моделювання знань (≈95 %), оскільки дозволяють підтримувати логічну узгодженість навіть за умови масштабування чи розширення структури. *Інтерпретованість* онтологій також залишається високою (≈85 %) завдяки їх семантичній прозорості та відповідності логіці предметної області, особливо для підготовлених користувачів. Разом з тим, рівень *актуалізації* (≈70 %) дещо нижчий порівняно з іншими підходами, оскільки внесення змін до онтологій потребує залучення експертів, а сама структура менш гнучка до динамічних змін.

Продукційні правила [31] є поширеним засобом представлення процедурних або евристичних знань, зокрема в експертних системах. Завдяки модульній природі, продукційні правила забезпечують високий рівень *структурованості* знань (≈80 %) — кожне правило є незалежною умовно-наслідковою конструкцією, що полегшує додавання нової інформації та локальне оновлення.

Ключовою перевагою таких систем є прозорість логіки виведення й можливість трасування процесу формування висновків, що зумовлює високий рівень *інтерпретованості* (≈95 %). Проте *актуалізація* знань у великих базах знань ускладнюється, оскільки збільшення кількості правил призводить до зниження керованості та потребує значних зусиль з боку експертів для підтримання консистентності (≈65 %). На відміну від онтологій, *нормалізація* знань у правилах досягається за рахунок повторного використання структур шаблонів і модифікованих блоків знань (≈85 %), хоча загальна формалізація може бути нижчою. Щодо *стабільності*, то бази продукційних правил демонструють помірні результати (≈75 %): хоча модифікація одного правила не впливає безпосередньо на інші, проте відсутність централізованої структури призводить до ризику їх дублювання або суперечливості.

Фрейми [30] демонструють високий рівень *структурованості* (≈90 %) завдяки чітко визначеній ієрархії та механізму спадкування, що забезпечує узгоджене представлення знань у домені. Показник *актуалізації* також перебуває на середньому рівні (≈70 %), оскільки модульність фреймів дозволяє оновлювати окремі елементи без втручання у всю систему. Водночас, надмірна залежність між пов'язаними фреймами може призводити до каскадних змін, що дещо ускладнює підтримку консистентності. Ключовою перевагою є висока *інтерпретованість* (≈85 %) завдяки схожості фреймової моделі до людської організації пам'яті, що полегшує розуміння структури знань як розробниками, так і кінцевими користувачами. Щодо *нормалізації*, фрейми показують відносно високий результат (≈80 %), оскільки дозволяють узгоджувати різні типи знань, однак поступаються онтологіям за рівнем формалізації та аксіоматизації. Оцінка *стабільності* (≈85 %) вказує на доволі надійну підтримку вже побудованих ієрархій, однак необхідність перегляду структури при додаванні нових типів об'єктів або зв'язків обумовлює ризики втрати сумісності з існуючою базою знань.

Семантичні мережі [31] використовують графову модель для представлення асоціативних знань і характеризуються високою гнучкістю у моделюванні різноманітних зв'язків між концептами. Відсутність жорстких обмежень на типи об'єктів та відносин дозволяє ефективно відображати складні залежності, проте водночас знижує *структурованість* (≈65 %), оскільки мережа не завжди має чітко визначену ієрархію чи формалізовану схему. *Інтерпретованість* семантичних мереж залишається на середньому рівні (≈70 %) — візуалізація зв'язків є зручною, але контекстуальне значення деяких відношень може бути неоднозначним. Завдяки гнучкості структури, семантичні мережі забезпечують відносно середню *актуалізацію* знань (≈75 %): нові вузли й зв'язки можуть додаватися швидко, хоча це може впливати на загальну цілісність моделі. *Нормалізація* знань (≈65 %) є обмеженою через нестачу єдиної онтологічної основи, що ускладнює інтеграцію даних з різних джерел і формалізацію правил. Щодо *стабільності* (≈60 %), то додавання або зміна елементів мережі може призвести до суттєвих змін у взаємозв'язаних частинах графа, що вимагає постійного контролю за узгодженістю.

Підхід до організації знань на основі ***штучних нейронних мереж*** демонструє значний потенціал в системах кіберзахисту, особливо в контексті обробки великих обсягів гетерогенних даних у режимі реального часу. Завдяки здатності моделювати нелінійні залежності та виявляти приховані закономірності, нейромережі ефективно вирішують завдання класифікації, виявлення аномалій і прогнозування. Однак *структурованість* знань у таких моделях є низькою (≈40 %), оскільки знання зберігаються у вигляді числових ваг без явної логічної структури. *Інтерпретованість* також залишається обмеженою (≈30 %): більшість рішень нейромереж є «чорними скриньками», що ускладнює аналіз причин помилок і валідацію результатів. *Актуалізація* знань (≈80 %) здійснюється через донавчання моделей на нових даних, проте цей процес супроводжується ризиками перенавчання або втрати важливих раніше засвоєних патернів, особливо у відсутності якісних даних і чітко визначених обмежень. *Нормалізація* (≈50 %) є досить слабкою: не оперують чітко структурованими поняттями, що обмежує їхню здатність до інтеграції знань з формалізованих джерел. Щодо *стабільності* (≈60 %), нейромережі чутливі до зміни вхідних параметрів і особливостей навчальної вибірки, що може суттєво вплинути на результати, навіть за незначних змін у даних.

Проведений аналіз свідчить про те, що кожний з розглянутих підходів до організації знань має свої унікальні переваги та обмеження, які зумовлюють доцільність їх використання залежно від завдань, що стоять перед ІСК. Найбільший потенціал щодо відповідності зазначеним вимогам демонструє ***онтологічний*** підхід. До того ж, саме в онтологіях здатність до концептуального відображення історичних знань з можливістю динамічного оновлення вдало поєднується із зрозумілістю моделі знань для людини, що є важливою передумовою для ухвалення обґрунтованих рішень та

впровадження ефективних політик кіберзахисту. Обмеження цього підходу в контексті швидкості актуалізації знань зумовлюють доцільність інтеграції онтологій з іншими підходами з метою досягнення балансу між точністю, інтерпретованістю та оперативністю оновлення знань в ІСК.

Оскільки наступними ключовими викликами для управління знаннями в ІСК є семантичний бар'єр між джерелами даних та обмежена інтероперабельність форматів, подальший аналіз зосереджено на підходах до **інтеграції отриманих знань** за такими критеріями [32]—[36]: *формалізація*, *адаптивність*, *стандартизація*, *інтероперабельність*, *обчислювальна складність*, *гнучкість*, *концептуалізація*.

На рис. 3 показано результати порівняльного аналізу підходів до інтеграції знань в ІСК за описаними критеріями, що відображає рівень відповідності кожного підходу у відсотках.

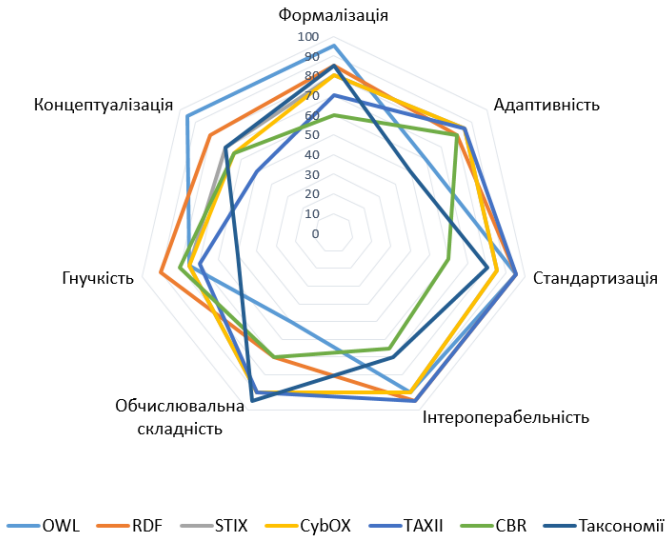

Рис. 3 Результати порівняльного аналізу підходів до інтеграції знань в ІСК

OWL (Web Ontology Language) [34] є частиною технології Semantic Web — концепції розвитку Всесвітньої павутини і мережі Інтернет. Завдяки потужній здатності до формалізації та концептуалізації гетерогенних даних OWL дозволяє створювати та підтримувати в актуальному стані точні та однозначні онтологічні моделі знань стосовно семантики мережевих топологій, характеристик пристроїв, потоків інформації, вразливостей та сценаріїв кіберзагроз. OWL демонструє високі значення за ключовими критеріями інтеграції знань: *формалізація* — 95 %, концептуалізація — 95 %, стандартизація — 95 %, інтероперабельність — 90 %, що свідчить про її придатність для формального, однозначного та структурованого подання знань у сфері кібербезпеки. Водночас, показник обчислювальної складності 90 % вказує на значні вимоги до ресурсів, особливо у разі масштабування онтологій та виконання логічного виведення. За показниками гнучкості — 75 % та адаптивності — 60 %, OWL має деякі обмеження щодо динамічного оновлення знань та адаптації до нових типів загроз у режимі реального часу.

RDF (Resource Description Framework) [34] є основою концепції Semantic Web, побудованою на основі веб-стандартів (XML, Turtle, JSON-LD, N-Triples) і призначеною для представлення знань у вигляді орієнтованих графів знань. У відповідності до результатів порівняльного аналізу, RDF демонструє високі показники за критеріями: *інтероперабельність* — 95 %, *стандартизація* — 95 %, що забезпечує його широку сумісність із сучасними платформами та безперешкодну інтеграцію у гетерогенні інформаційні системи. До того ж, RDF характеризується високим рівнем *гнучкості* — 90 % та *адаптивності* — 80 %, що дає змогу ефективно оновлювати і масштабувати знання у динамічному середовищі кіберпростору. За критеріями *формалізації* — 85 % та *концептуалізації* — 80 %, RDF є потужним засобом опису структурованих даних, проте для моделювання складних семантичних зв'язків часто потребує використання розширень, таких як OWL. Водночас, *обчислювальна складність* — 70 % залишається помірною, через що RDF придатна для швидкої обробки великих обсягів метаданих, зокрема в завданнях кіберрозвідки, обміну загрозами та підвищення рівня кіберситуаційної обізнаності.

STIX (Structured Threat Information Expression) [35] — структурована мова представлення інформації про кіберзагрози у форматі JSON, яка характеризується високими показниками *формалізації* (≈80 %), *стандартизації* (≈85 %) та *інтероперабельності* (≈90 %), що забезпечує її широке застосування в інфраструктурах обміну інформацією про загрози, зокрема у взаємодії між ІСК, платформами обробки індикаторів компрометації. *Гнучкість* (≈75 %) та *адаптивність* (≈85 %) свідчать про достатню здатність STIX до адаптації моделей знань під специфіку організацій або сценаріїв реагування на загрози. Проте, *концептуалізація* (≈70 %) обмежує рівень абстрактного подання знань, оскільки STIX зосереджений переважно на фіксації вже відомих сутностей, індикаторів, тактик і технік. *Обчислювальна складність* (≈90 %) зумовлена детальною структурою та

взаємозалежністю STIX-об'єктів, що підвищує вимоги до ресурсів при їх обробці, зокрема в реальному часі.

CybOX (Cyber Observable eXpression) [33] — стандартизована мова для кодування та обміну високоякісною інформацією про кіберспостереження. Завдяки модульній багаторівневій структурі підхід адаптований для ефективної обробки великих обсягів даних без значних обчислювальних ресурсів. Згідно з результатами порівняльного аналізу, підхід характеризується такими показниками: *адаптивність* — 85 %, *інтероперабельність* — 90 %, *стандартизація* — 85 %, *гнучкість* — 75 %, що забезпечує його гнучке впровадження в інструментах цифрової криміналістики та системах моніторингу. Разом з цим, *формалізація* — 80 % та *концептуалізація* — 65 % свідчать про обмежену здатність CybOX до побудови глибоких семантичних моделей — мова зосереджена на описі окремих подій та об'єктів, а не на їх концептуальних взаємозв'язках. *Обчислювальна складність* — 90 % є високою, що зумовлено детальністю моделі та необхідністю обробки великої кількості атрибутів і взаємозалежностей.

TAXII (Trusted Automated eXchange of Indicator Information) [36] — транспортний протокол і набір сервісів для безпечного та автоматизованого обміну повідомленнями про кіберзагрози. Функціонує як універсальний засіб передачі структурованих даних, зокрема у форматі **STIX**. Згідно з результатами порівняльного аналізу, TAXII має такі показники: *інтероперабельність* — 95 %, *стандартизація* — 95 %, тому він є сумісним з більшістю сучасних рішень у сфері обміну знаннями. *Гнучкість* — 75 % та *адаптивність* — 85 % свідчать про високу здатність протоколу до інтеграції у наявні процеси без необхідності значних змін в інфраструктурі. Однак, TAXII не є засобом семантичного моделювання знань, що відображено значеннями таких критеріїв: *формалізація* — 70 %, *концептуалізація* — 50 %, оскільки структура та зміст переданих даних повністю залежать від використовуваних форматів, а не самого протоколу. *Обчислювальна складність* — 90 % є досить високою, що пов'язано з обробкою складних структур даних, підтримкою різних режимів передачі та вимогами до захищеного транспортування.

CBR (Case-Based Reasoning) [32] — метод пошуку та адаптації рішень на основі ретроспективного аналізу кіберінцидентів засобами технологій ШІ. Забезпечує накопичення знань у вигляді кейсів — описів раніше вирішених ситуацій із застосуванням до нових, подібних випадків. За результатами порівняльного аналізу, CBR характеризується такими показниками: *адаптивність* — 80 %, *гнучкість* — 80 %, що пояснюється здатністю ефективно працювати в умовах неповних, неточних або змінюваних вхідних даних, властивих сучасному кіберсередовищу. Водночас, *концептуалізація* — 65 %, *формалізація* — 60 %, залежать від обраного способу представлення кейсів (від неструктурованого тексту до формалізованих шаблонів). Через відсутність галузевого стандарту, CBR-системи мають обмежену *стандартизацію* — 60 % та *інтероперабельність* — 65 %, що ускладнює обмін кейсами між різними реалізаціями. *Обчислювальна складність* — 70 % лишається на середньому рівні, зростає зі збільшенням бази знань або складністю механізмів подібності, проте загалом залишається прийнятною для практичного використання.

Таксономії [34] — ієрархічні системи класифікації, що використовуються для організації та категоризації сутностей у сфері кібербезпеки на основі заздалегідь визначених критеріїв. Широко застосовуються для опису кібератак, типів загроз, вразливостей та інцидентів, зокрема в системах виявлення вторгнень, при оцінці ризиків і плануванні заходів протидії. Згідно з результатами порівняльного аналізу, таксономії демонструють: *формалізація* — 85 %, *стандартизація* — 80 %, *інтероперабельність* — 70 %, що свідчить про їх відносно високий рівень структурованості та поширення в індустрії. Разом з тим, за критеріями: *гнучкості* — 50 %, *адаптивності* — 50 %, *концептуалізації* — 70 %, підхід демонструє певні обмеження, зокрема переважна фіксація відомих категорій об'єктів та подій, недостатня адаптація до нових, нестандартних кіберзагроз. *Обчислювальна складність* — 95 % є найвищою серед усіх розглянутих підходів, що зумовлено потребою в глибокій обробці ієрархічних структур, великої кількості категорій та залежностей між ними, особливо у разі масштабного впровадження.

Проведений порівняльний аналіз підходів до інтеграції знань у сфері кібербезпеки демонструє суттєві відмінності між ними за розглянутими критеріями. Найдоцільнішим підходом до інтеграції знань в онтології є використання технологій Semantic Web, зокрема поєднання OWL з RDF (за потреби доповненням стандартами RDFS), оскільки забезпечить високий рівень формалізації, насичену концептуалізацію та гнучку інтеграцію гетерогенних даних, що є ключовими факторами створення комплексних і точних моделей знань у сфері кібербезпеки.

Не менш важливою фазою управління знаннями в ІСК є вибір підходів до їх отримання. Необ-

хідність аналізу таких підходів обумовлена мінімізацією часу від появи інформації про кіберзагрозу до моменту реагування на неї, масштабованістю системи, відповідністю знань нормативним припущенням і стандартам кіберзахисту, а також наявністю механізмів верифікації. У зв'язку з цим, порівняльний аналіз підходів до **здобування знань** в ІСК доцільно здійснювати за такими критеріями [37]—[39]: *оперативність, масштабованість, передбачуваність, потреба у верифікації.*

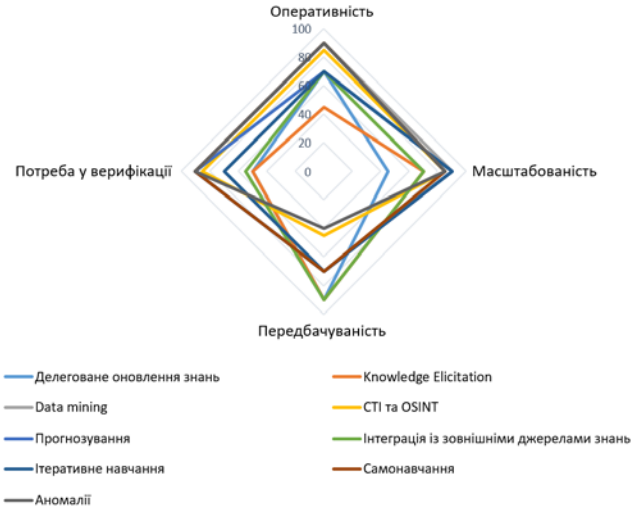

Рис. 4. Результати порівняльного аналізу підходів до здобування знань для ІСК

На рис. 4 показано результати порівняльного аналізу підходів до видобутку знань за описаними критеріями, що відображає рівень відповідності кожного підходу у відсотках.

Актуалізація моделі знань передбачає проходження повного циклу: від ідентифікації релевантних джерел у просторі та часі до формалізованого представлення нових знань, що можуть бути інтегровані в наявну структуру.

Делеговане оновлення знань [38] передбачає, що підготовка, тестування та розповсюдження оновлень безпеки покладається на постачальників програмного забезпечення, що породжує залежність від термінів оновлень, які надходять від конкретного постачальника, і, відповідно, обмежує *оперативність* (≈70 %) та *масштабованість* (≈45 %). Проте отримані знання мають високий кредит довіри, наданий у разі вибору постачальника, що забезпечує високу *передбачуваність* (≈90 %) та усуває потребу в додатковій *верифікації* (≈50 %).

Вилучення знань (Knowledge Elicitation) [37] полягає в зборі, узагальненні та документуванні знань експертів, аналітиків, дослідників на основі їхнього досвіду, навичок та спеціалізації щодо методів кібератак, контрзаходів і процедур реагування на кіберінциденти. Цей підхід характеризується високою передбачуваністю (≈90 %) за рахунок участі досвідчених фахівців та достатньою масштабованістю (≈70 %), оскільки збільшення кількості експертів або документації значно ускладнює координацію процесу отримання знань. *Оперативність* є відносно низькою (≈45 %) через значні часові витрати, особливо за великого обсягу знань. *Потреба у верифікації* становить (≈50 %) і зумовлена ризиками суб'єктивності та упередженості експертних суджень.

Інтелектуальний аналіз даних (Data mining) [39] полягає у застосуванні методів обробки природної мови, машинного та глибокого навчання для виявлення неочевидних, об'єктивних, корисних на практиці закономірностей та аномалій, що демонструють найвищі показники *оперативності* (≈90 %) та *масштабованості* (≈90 %) серед розглянутих підходів. *Передбачуваність* — (70 %) зумовлена достатньо стабільними результатами автономних моделей, проте їхня відповідність нормативним очікуванням може варіюватись залежно від якості навчальних даних і гіперпараметрів. Натомість *потреба у верифікації* є найвищою (≈90 %) через ризики включення недостовірних або нерелевантних знань, що потребують підтвердження достовірними джерелами або експертною оцінкою.

Інформація про кіберзагрози (Cyber Threat Intelligence, CTI) та розвідка з відкритих джерел (Open Source Intelligence, OSINT) [37] в контексті кібербезпеки представлений як збір та аналіз загальнодоступної інформації для розуміння ландшафту кіберзагроз та прийняття обґрунтованих рішень щодо застосування контрзаходів. Завдяки можливості налаштування інструментів з відкритим кодом під конкретні потреби в режимі реального часу *оперативність* та *масштабованість* оцінюється (≈85 %). Проте рівень *передбачуваності* значно нижчий за інші підходи (≈45 %), оскільки реальний кіберпростір сповнений невизначеностей, до того ж наявність потенційних ризиків безпеки, пов'язаних з відкритим характером платформ, вимагає детальної технічної експертизи отриманих знань для їх ефективного використання (≈85 %).

Прогнозування [38] є проактивним підходом, що передбачає отримання нових знань через симуляцію потенційних сценаріїв кібервпливу на основі результатів аудиту систем кіберзахисту та аналізу тенденцій розвитку поведінкових аспектів у сфері кіберзлочинності. Прогнозування має значний потенціал для отримання знань завчасно, до фактичного здійснення кібератак, проте фак-

тор невизначеності зумовлює середній рівень *передбачуваності* (≈70 %). Незважаючи на наявність відносно ефективних методів прогнозування, їх машинна реалізація дозволяє залучати широкий перелік джерел знань, що впливає на *масштабованість* (90 %), проте обсяги даних, які необхідно обробити, безпосередньо впливають на *оперативність* — 70 %. Через динамічність ландшафту кіберзагроз та непередбачуваність дій зловмисників, виникає значна *потреба у верифікації* (≈90 %) отриманих знань для забезпечення їх точності та релевантності.

Інтеграція з зовнішніми джерелами знань [39] (наприклад, MITRE ATT&CK, CVE, STIX/TAXII) дозволяє здійснювати автоматичне оновлення категорій кібератак, вразливостей та індикаторів компрометації. *Оперативність* отримання знань (≈70 %) є обмеженою через те, що нові знання часто мають ретроспективний характер, оскільки проходять певні етапи попередньої обробки та експертизи на стороні постачальника. Наявність обмеженої кількості стандартизованих загальнодоступних джерел знань знижує показник *масштабованості* (70 %). Враховуючи високий ступінь структурованості та атрибуції вже отриманих знань, *передбачуваність* даного підходу становить (≈90 %), а *потреба у верифікації* отриманих знань (≈55 %).

Ітеративне навчання [39], як приклад комбінованого людино-машинного підходу, за якого система автоматично виявляє взаємозв'язки між сутностями у моделі знань та звертається до аналітиків або експертів для їх підтвердження чи уточнення. Підхід характеризується високою *масштабованістю* (≈90 %) за рахунок застосування автоматизованих методів видобутку знань, проте наявність людини в циклі, з одного боку знижує показник *оперативності* — 70 %, через потребу часових ресурсів для якісного аудиту, а з іншого підвищує *передбачуваність* — 70 %, оскільки досвід та кваліфікація експерта має певний кредит довіри. *Потреба у верифікації* — 70 % залишається на середньому рівні у зв'язку з тим, що автоматизовані методи видобутку знань створюють певний рівень інформаційного шуму.

Самонавчання [37] передбачає використання адаптивних алгоритмів для автономного оновлення моделі знань у реальному часі. Це забезпечує обробку великих обсягів різнорідних даних і високу *оперативність* (≈90 %) завдяки ефективній роботі конвеєрів обробки подій та автоматичному оновленню правил на основі навчання з підкріпленням. *Масштабованість* (≈85 %) досягається завдяки гнучкому підключенню нових джерел даних (телеметрія, журнали, OSINT) без потреби ручного втручання, що підтримується механізмами data fusion і semantic enrichment. Модель знань має модульну структуру (knowledge graph), яка динамічно доповнюється, а online learning забезпечує її адаптацію під час експлуатації. *Передбачуваність* (≈70 %) є середньою й залежить від налаштування відповідності стандартам (ISO, NIST). *Потреба у верифікації* (≈90 %) зумовлена ризиками помилкових або шкідливих оновлень, тому інтеграція нових знань супроводжується перевіркою релевантності та достовірності джерел.

Аномалії [38] відхилення від очікуваної поведінки в системах, мережах або даних, які можуть свідчити як про нові кіберзагрози, так і про внутрішні збої. *Оперативність* (≈90 %) досягається завдяки потоковій аналітиці, обробці даних в оперативній пам'яті та швидкій активації контрзаходів на основі виявлених індикаторів компрометації в межах допустимого часу реагування, визначеного угодою про рівень сервісу. *Масштабованість* (≈85 %) забезпечується гнучкою архітектурою та можливістю інтегрувати численні потоки даних і сховища. *Передбачуваність* є низькою (≈40 %), оскільки автоматичне виявлення аномалій часто не узгоджується з нормативними моделями та політиками безпеки, що не встигають за динамікою загроз. *Потреба у верифікації* надзвичайно висока (≈95 %) через ризик хибних спрацьовувань, що потребує додаткової перевірки релевантності виявлених подій.

Оцінка наявних підходів до видобутку знань для ІКС демонструє їх суттєві відмінності за фокусом: одні орієнтовані на швидкість та масштаб, тоді як інші на контрольовану якість і довіру до джерел. Жоден з них не забезпечує повної відповідності всім вимогам одночасно, що підкреслює об'єктивну потребу в інтеграції гібридних стратегій отримання знань, де автоматизовані методи доповнюються експертною оцінкою, а гнучкість механізмами перевірки.

Таким чином, проведений поетапний аналіз підходів до управління знаннями в ІСК виявив наявність суттєвих розбіжностей між існуючими методами за критеріями структурованості, актуалізації, інтерпретованості, інтеграції, оперативності та передбачуваності. Жоден з проаналізованих підходів не забезпечує повної відповідності всім вимогам, що ускладнює створення ефективної, адаптивної та прозорої системи знань для потреб кібербезпеки, що обґрунтовує розробку нових гібридних моделей управління знаннями, здатних інтегрувати переваги різних підходів, зберігаючи баланс між формалізацією, гнучкістю, інтероперабельністю та прозорістю прийняття рішень в

умовах динамічного кіберсередовища.

Враховуючи виявлені обмеження наявних підходів до реалізації життєвого циклу управління знаннями в ІСК, доцільним напрямком подолання зазначених викликів є розробка науково-методичного апарату управління знаннями, який дасть змогу поєднати високий ступінь їх формалізації та структурованості на основі онтологій з динамічними механізмами самонавчання та оновлення знань в режимі реального часу.

Так, запропоновано підхід до управління знаннями в ІСК, який поєднує онтологічне ядро зі здатністю до адаптації на основі самонавчання та механізмів верифікації. Узагальнену функціональну схему цього підходу показано на рис. 5.

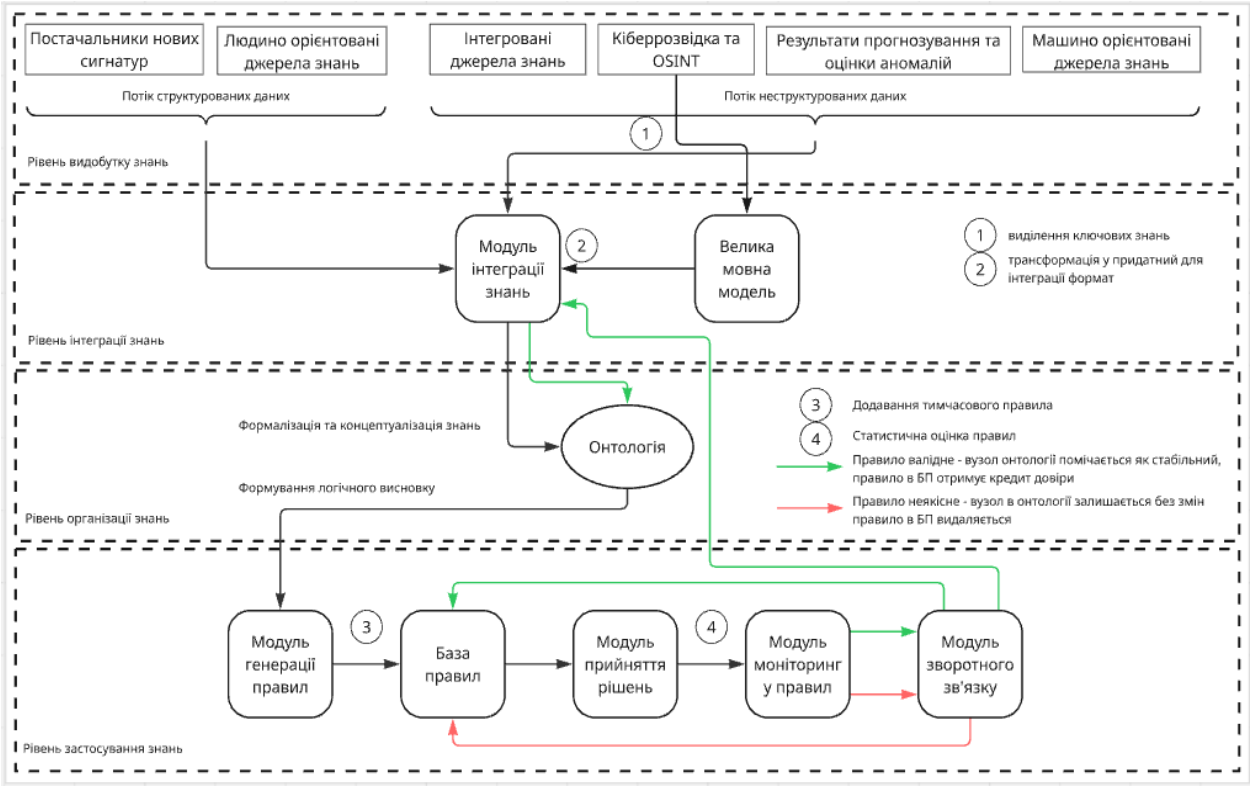

Рис. 5. Узагальнена функціональна схема реалізації життєвого циклу процесу управління знаннями в ІСК

Запропонована функціональна схема відображає багаторівневу архітектуру управління знаннями в ІСК, що охоплює повний цикл роботи з даними від моменту надходження інформації з різнорідних джерел до її формалізації, інтеграції, організації у вигляді онтологічної моделі та подальшого практичного застосування у вигляді правил прийняття рішень. Кожний рівень архітектури пов’язаний з відповідними модулями, які взаємодіють між собою в межах єдиного циклу оновлення та верифікації знань.

На рівні **здобування знань** процес починається з консолідації розширеного переліку альтернативних джерел, як структурованих (сигнатури, аналітичні звіти, машинно орієнтовані джерела), так і неструктурованих (OSINT, результати прогнозування) з метою забезпечення належного рівня ситуаційної обізнаності.

Ключовим компонентом цього рівня є конвеєр обробки природної мови на базі великої мовної моделі, який виконує токенізацію, лематизацію, розпізнавання сутностей та виявлення відношень між ними, трансформуючи текстові дані у формат, придатний для подальшої інтеграції. Data Mining інструменти застосовуються для виявлення неочевидних закономірностей і аномальних патернів, а OSINT-агенти для автоматизованого парсингу відкритих джерел. Для забезпечення потокової обробки даних у реальному часі можуть бути використані такі технології, як Apache Kafka у поєднанні з Flink або Spark Streaming, що дозволяє досягти низької затримки у разі надходження нових знань до ІСК.

Рівень **інтеграції знань** передбачає застосування ефективних ETL-оркестраторів, які призначені для уніфікації гетерогених даних у єдиний RDF/OWL формат, що в свою чергу забезпечує семантичну узгодженість, структурованість та логічну несуперечність отриманих знань.

На рівні **організації знань** реалізується формалізація та концептуалізація даних у вигляді онтологічних структур, які є основою для подальшого автоматизованого виведення знань і прийняття рішень.

Рівень **застосування знань** включає модуль генерації правил, який на основі онтологічної моделі та за допомогою алгоритмів індукції виявляє патерни загроз і формулює умовно-дієві конструкції, автоматично наповнюючи шаблони правил з урахуванням контекстних атрибутів активів і CVSS-метрик. Згенеровані правила надходять до бази правил, де кожне отримує початковий «кредит довіри» на основі статистичної оцінки історичних кейсів. Надалі правила підлягають валідації, і в разі визнання їх коректними — закріплюються як валідні, інакше — видаляються. Модуль прийняття рішень взаємодіє з модулем моніторингу правил, який оцінює їхню ефективність у реальному середовищі. Якщо виявлено зниження продуктивності або суперечності, модуль зворотного зв'язку ініціює оновлення «кредиту довіри» та адаптацію правила через механізми active learning і експертну верифікацію, забезпечуючи тим самим безперервне вдосконалення та самонавчання ІСК.

Висновок

Проведено системний поетапний аналіз сучасних підходів до реалізації життєвого циклу управління знаннями в ІСК, що охоплює фази видобутку, організації, інтеграції та застосування знань. Встановлено, що жоден з наявних підходів не забезпечує повної відповідності всім ключовим вимогам, таким як структурованість, актуалізація, інтерпретованість, масштабованість, гнучкість та прозорість прийняття рішень, що ускладнює створення ефективної системи знань для потреб кібербезпеки. Найбільший потенціал у контексті формалізації та структурованості продемонстровано онтологічним підходом, тоді як найоперативнішими є методи самонавчання та Data mining. Водночас, саме гібридні стратегії, що інтегрують сильні сторони різних підходів, дозволяють досягти балансу між точністю, швидкістю оновлення та адаптивністю до нових загроз.

У відповідь на виявлені виклики запропоновано функціональну схему управління знаннями в ІСК, що поєднує онтологічну модель з самонавчальними та верифікаційними механізмами. Запропонований підхід забезпечує наскрізну обробку даних від видобутку знань до їхнього практичного застосування у вигляді адаптивних захисних політик. Зазначене створює підґрунтя для розробки ІСК нового покоління, здатних до автономного вдосконалення, прийняття обґрунтованих рішень та забезпечення високої кіберстійкості ІКС в умовах динамічного кіберсередовища.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] V. Fesokha, "Peculiarities of the confrontation between defensive and offensive artificial intelligence in cyberspace," *International Science Journal of Engineering & Agriculture*, vol. 3, no. 4, pp. 105-114, 2024. [Electronic resource]. Available: https://isg-journal.com/isjea/article/view/764/ .

[2] L. Jiang, A. Jayatilaka, M. Nasim, M. Grobler, M. Zahedi, M. A. Babar, "Systematic Literature Review on Cyber Situational Awareness Visualizations," *IEEE Access*, vol. 10, pp. 57525-57554, 2022. https://doi.org/ 10.1109/ACCESS.2022.3178195 .

[3] CERT-UA. *Порівняльний аналіз ШПЗ WhisperKill та WhiteBlackCrypt*. [Electronic resource]. Available: https://cert.gov.ua/article/18108 .

[4] CERT-UA. Наступна кібератака групи Sandworm (UAC-0082) на об'єкти енергетичної інфраструктури України. [Electronic resource]. Available: https://cert.gov.ua/article/39518 .

[5] CERT-UA. *Публічні PGP-ключі CERT-UA*. https://doi.org/ https://cert.gov.ua/article/38088 .

[6] "SentinelLabs. 12 Months of Fighting Cybercrime & Defending Enterprises," *SentinelLabs 2024 Review*. [Electronic resource]. Available: https://strategicfocus.com/2025/01/02/12-months-of-fighting-cybercrime-defending-enterprises-sentinellabs-2024-review .

[7] L. F. Sikos, "Cybersecurity knowledge graphs," *Knowledge and Information Systems*, vol. 65, no. 3. pp. 789-812, 2023, https://doi.org/ 10.1007/s10115-023-01860-3 .

[8] MITRE ATT&CK®. *A knowledge base of adversary tactics and techniques*. [Electronic resource]. Available: https://attack.mitre.org .

[9] STIX Project. *Structured Threat Information eXpression (STIX™)*. [Electronic resource]. Available: stixproject.github.io .

[10] S. Fenz, A. Ekelhart, "A cybersecurity ontology to support risk information gathering in early phases of the system development life cycle," *Advances in Information and Computer Security. Springer*, pp. 13-26, 2021. https://doi.org/10.1007/978-3-030-95484-0_2 .

[11] D Wu., J. Chen, R. Xie, et al. "OntoCSD: an ontology-based security model for an integrated solution of cyberspace defense," *Frontiers of Information Technology & Electronic Engineering*, vol. 25, no. 9, pp. 1209-1225, 2024. https://doi.org/10.1631/FITEE.2300662 .

[12] I. H. Sarker, H. Janicke, M. A. Ferrag, and A. Abuadbba, "Multi-aspect rule-based AI: Methods, taxonomy, challenges and directions towards automation, intelligence and transparent cybersecurity modeling for critical infrastructuresб" *Internet of Things*, vol. 25, 2024, *Article 101110*. https://doi.org/10.1016/j.iot.2024.101110 .

[13] A. Alshamrani, S. Myneni, A. Chowdhary, and D. Huang, “A hybrid approach using support vector machine rule-based system for cyber threat detection in IoT,” *Scientific Reports*, vol. 14, 2024. Article 78976. https://doi.org/10.1038/s41598-024-78976-1.

[14] Y. Zhang, L. Wang, and J. Li, “A review of knowledge graph application scenarios in cyber security,” *arXiv preprint*, 2022. arXiv:2204.04769.[Electronic resource]. Available: https://arxiv.org/abs/2204.04769 .

[15] D. Pérez, J. García, and M. López, “Rule-based with machine learning IDS for DDoS attack detection in SDN environments,” *IEEE Access*, vol. 12, pp. 12345-12356, 2024. https://doi.org/10.1109/ACCESS.2024.10638035 .

[16] S. Dotsenko, O. Illiashenko, S. Kamenskyi, and V. Kharchenko, “Integrated model of knowledge management for security of information technologies: standards ISO/IEC 15408 and ISO/IEC 18045,” *Information & Security: An International Journal*, vol. 43, no. 3, pp. 305-317, 2019.[Electronic resource]. Available: https://connections-qj.org/article/integrated-model-knowledge-management-security-information-technologies-standards-isoiec .

[17] N. Sun, et al., “Cyber Threat Intelligence Mining for Proactive Cybersecurity Defense: A Survey and New Perspectives,” *IEEE Communications Surveys & Tutorials*, vol. 25, no. 3, pp. 1748-1774, 2023. https://doi.org/10.1109/COMST.2023.3273282 .

[18] D. Tayouri, S. Hassidim, A. Smirnov, and A. Shabtai, *Cybersecurity in Agile Cloud Computing—Cybersecurity Guidelines for Cloud Access. IEEE White Paper*, 2022, 22 p. [Electronic resource]. Available: https://ieeexplore.ieee.org/document/9904636 .

[19] P. Podder, S. Bharati, M.R.H. Mondal, P.K. Paul, and U. Kose, “Artificial Neural Network for Cybersecurity: A Comprehensive Review,” *Journal of Information Assurance & Security*, vol. 16, no. 1, pp. 10-23, 2021.[Electronic resource]. Available: https://arxiv.org/pdf/2107.01185 .

[20] I. Akour, M. Alauthman, K.M.O. Nahar, A. Almomani, and B. B. Gupta, “Analyzing Darknet Traffic Through Machine Learning and Neucube Spiking Neural Networks,” *Intelligent and Converged Networksm*, vol. 5, no. 4, pp. 265-283, 2024. https://doi.org/10.23919/ICN.2024.0022.

[21] Univerzita obrany / Czech Republic. *18th PhD Conference Proceedings: New Approaches to State Security Assurance.* – Brno: University of Defence, 2024. ISBN 978-80-7582-512-4.

[22] Llopis Sánchez S, *Decision support elements and enabling techniques to achieve a cyber defence situational awareness capability*. Valencia: Universitat Politècnica de València, 2023, 107 p. https://doi.org/10.4995/Thesis/10251/194242. [Electronic resource]. Available: https://riunet.upv.es/handle/10251/194242 .

[23] N. R. Vajjhala, and K. D. Strang, *Cybersecurity in Knowledge Management: Cyberthreats and Solutions.* – London: Routledge, 2024,256 p.

[24] J. Wei, “Knowledge management framework for cyber security learning,” *International Journal of Management in Education*, vol. 4, no. 1, pp. 95-106,2010. https://doi.org/ 10.1504/IJMIE.2010.029884 .

[25] *ISO 30401:2018 Knowledge management systems — Requirements*. – Geneva: International Organization for Standardization, 2018, 20 p. https://doi.org/10.1002/9781119027769.ch4 .

[26] IBM. *Machine Learning Analytics app – IBM QRadar Documentation.* [Electronic resource]. Available: https://www.ibm.com/docs/en/qradar-common?topic=app-machine-learning-analytics .

[27] Elastic. *Elastic Security for SIEM* . [Electronic resource]. Available: https://www.elastic.co/security/siem .

[28] Microsoft. *Bring your own Machine Learning (ML) into Microsoft Sentinel* [Electronic resource]. Available: https://learn.microsoft.com/en-us/azure/sentinel/bring-your-own-ml .

[29] В. Фесьоха, і І. Субач, «Принципи забезпечення кіберстійкості інформаційно-комунікаційних систем на основі технологій штучного інтелекту,» *Проблеми кібербезпеки інформаційно-комунікаційних систем*, тези доповідей VIII Міжнародної науково-практичної конференції, 11 квітня 2025 р., Київ, Україна. Київ, 2025, с. 56-57.

[30] ISKO UK. *Knowledge organization: introductory publications.* [Electronic resource]. Available: https://www.iskouk.org/knowledge-organization-introductory-publications .

[31] B. Hjørland, “Theories of knowledge organization,” in *Introduction to Knowledge Organization. – Cambridge University Press*, pp. 70-90, 2020. [Electronic resource]. Available: https://www.cambridge.org/core/books/abs/introduction-to-knowledge-organization/theories-of-knowledge-organization/70CAB48C676B089843B7F82D75C7ECDD .

[32] M. E. Said, and M.A. Jabar, “Knowledge Integration Framework: A Systematic Review,” I*nternational Journal of Computer Applications*, vol. 182, no. 2, pp. 1-8, 2023. https://doi.org/10.5120/ijca2023922345 .

[33] A. Scharnhorst, R. P. Smiraglia, “The Need for Knowledge Organization,” *Linking Knowledge: Linked Open Data for Knowledge Organization*, Eds. R. P. Smiraglia, A. Scharnhorst. Baden-Baden: Ergon Verlag, 2021, pp. 1-23. https://doi.org/10.5771/9783956506611-1 .

[34] B. Bayerlein, M. Schilling, P. von Hartrott, and J. Waitelonis, “Semantic integration of diverse data in materials science: Assessing Orowan strengthening,” *Scientific Data*, vol. 11, 2024, Article No. 434. https://doi.org/10.1038/s41597-024-03169-4.

[35] *OASIS. STIX™ Version 2.1*. [Electronic resource]. Available: https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.pdf

[36] *OASIS. TAXII™ Version 2.1.* [Electronic resource]. Available: https://docs.oasis-open.org/cti/taxii/v2.1/os/taxii-v2.1-os.html .

[37] Y. Chasseray, A.-M. Barthe-Delanoë, S. Négny, and J.-M. Le Lann, “Knowledge extraction from textual data and performance evaluation in an unsupervised context,” *Information Science.*, vol. 629, pp. 324-343, 2023. https://doi.org/10.1016/j.ins.2023.01.150 .

[38] H. Kim, L. He, and Y. Di, “Knowledge Extraction Framework for Building a Largescale Knowledge Base,” E*AI Endorsed Transactions on Industrial Networks and Intelligent Systems*, vol. 3, no. 7, 2016. https://doi.org/0.4108/eai.21-4-2016.151157.

[39] F. Seitl, T. Kovářík, et al., “Assessing the quality of information extraction,” *arXiv preprint*, arXiv:2404.04068, 2024. https://doi.org/10.48550/arXiv.2404.04068 .

Рекомендована кафедрою менеджменту та безпеки інформаційних систем, ВНТУ

Стаття надійшла до редакції 5.06.2025

Фесьоха Віталій Вікторович — д-р філософії, доцент, докторант науково-організаційного відділу;

Легкобит Володимир Сергійович — ад'юнкт науково-організаційного відділу, e-mail: ab1250119@gmail.com ;

Романенко Сергій Олексійович — викладач кафедри комп'ютерних інформаційних технологій.
Військовий інститут телекомунікацій та інформатизації ім. Героїв Крут, Київ;

Чернявський Роман Геннадійович — старший науковий співробітник.
Центральний науково-дослідний інститут Збройних Сил України, Київ

V. V. Fesokha[1]
V. S. Lehkobyt[1]
R. G. Cherniavskyi[2]
S. O. Romanenko[1]

Analysis of Approaches to the Implementation of the Knowledge Management Life Cycle in Intelligent Cyber Defense Systems

[1]Kruty Heroes Military Institute of Telecommunications and Information Technology, Kyiv;
[2]Central Research Institute of the Armed Forces of Ukraine, Kyiv

The article investigates the task of effective knowledge management in intelligent cyber defense systems in order to enhance their ability to detect, interpret and prevent modern cyber threats. It is substantiated that achieving a high level of their adaptability and situational awareness is possible only if full life cycle of knowledge management is implemented, which includes the stages of extraction, integration, organization, application and updating.

A comparative analysis of modern approaches to the implementation of the key phases of knowledge management in intelligent cyber defense systems is carried out. Particular attention is paid to the analysis of approaches to the organization of knowledge, such as ontological modeling, knowledge graphs, production rules, frames, neural network structures and semantic networks. Relevant knowledge representation languages, threat information exchange protocols, and knowledge mining tools are considered. The results obtained show that none of the approaches under consideration fully meets the defined criteria for effective knowledge management, in particular, structuredness, relevance, interpretability, scalability, flexibility, computational efficiency, and transparency of decision-making. In this regard, the expediency of creating a hybrid knowledge management architecture that combines the advantages of different approaches is substantiated.

Functional scheme is proposed that integrates the ontological core with modules for self-learning, automatic rule generation, verification, and feedback. The presented approach ensures end-to-end processing of knowledge from extraction to practical application in the form of informed decisions in real time. This creates the basis for building a new generation of intelligent cyber defense systems capable of self-improvement and sustainable response to threats in a dynamic cyber environment.

Keywords: knowledge management, intelligent cyber defense systems, artificial intelligence, information and communication systems, cyber threats, cyber resilience.

Fesokha Vitaliy V. — PhD, Associate Professor, Post-Doctoral Researcher of the Department of Scientific and Organizational;

Legkobit Vladimir S. — Adjunct of the Department of Scientific and Organizational, e-mail: ab1250119@gmail.com ;

Chernyavsky Roman G. — Senior Research Fellow;

Romanenko Sergii O. — Lecturer of the Chair of Computer Information Technologies