УДК 004.891:004.056.5 DOI: 10.31673/2412-4338.2026.019017

Розломій Інна Олександрівна
к.т.н., доц., доцент кафедри інформаційної безпеки та комп'ютерної інженерії
Черкаський державний технологічний університет, Черкаси
ORCID 0000-0001-5065-9004

Бабенко Віра Григорівна
д.т.н., проф., завідувач кафедри інформаційної безпеки ком'пютерної інженерії
Черкаський державний технологічний університет, Черкаси
Державний університет інформаційно-комунікаційних технологій, Київ
ORCID 0000-0003-2039-2841

Головня Вікторія Мілентівна
старший викладач кафедри прикладної радіоелектроніки
КПІ ім. Ігоря Сікорського, Київ
ORCID 0000-0001-7979-1412

ОНТОЛОГІЧНА ЕКСПЕРТНА СИСТЕМА ДЛЯ ВИЗНАЧЕННЯ ВРАЗЛИВИХ КОМПОНЕНТІВ У СИСТЕМАХ БЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧОЇ ІНФРАСТРУКТУРИ

Анотація: *У статті представлено онтологічну експертну систему, призначену для автоматизованого виявлення вразливих компонентів у системах безпеки об'єктів критичної інфраструктури. Рішення побудовано на основі використання онтологій як формального засобу подання знань, що дозволяє семантично описувати структуру системи, типи загроз, можливі вектори атак, наслідки компрометації та відповідні контрзаходи. На відміну від традиційних методів аналізу, що зазвичай використовують фіксовані правила або ручну інтерпретацію ризиків, онтологічна модель забезпечує логічне виведення нових знань на основі взаємозв'язків між об'єктами, враховуючи як структурні, так і контекстуальні залежності.*

Актуальність дослідження зумовлена складністю сучасних інфраструктурних систем і обмеженнями існуючих методів оцінювання, які не завжди дозволяють масштабувати модель, враховувати специфіку конкретного об'єкта або пояснювати отримані результати. Архітектура системи включає п'ять основних модулів: онтологічну базу знань (у форматі OWL), модуль логічного виведення на основі правил SWRL, інтерфейс користувача для введення даних і візуалізації результатів, базу даних вразливостей і загроз (зокрема CVE, STRIDE), а також модуль оновлення знань.

У межах кейс-стаді досліджено змодельований об'єкт енергетичної інфраструктури, що дозволило перевірити здатність системи виявляти складні ланцюги вразливостей з високою точністю. Було проаналізовано компоненти системи, виявлено програмне забезпечення з відомими вразливостями, ідентифіковано ризики та запропоновано рекомендації щодо їх усунення. Проведене тестування продемонструвало переваги онтологічного підходу порівняно з традиційним аналізом за такими критеріями, як точність, швидкість і пояснюваність результатів. Отримані результати підтверджують практичну цінність розробленої системи для підвищення стійкості об'єктів критичної інфраструктури до кібератак та обґрунтовують доцільність подальших досліджень у напрямі інтеграції з системами моніторингу та розширення онтологічної моделі.

Ключові слова: *онтологія, експертна система, вразливості, критична інфраструктура, логічне виведення, кібербезпека.*

Rozlomii Inna
PhD, Associate Professor,
Associate Professor of the Department of Information Security and Computer Engineering
Cherkasy State Technological Universit, Cherkasy
ORCID 0000-0001-5065-9004

Babenko Vira
Doctor of Technical Sciences, Professor,
Head of the Department of Information Security and Computer Engineering
Cherkasy State Technological Universit, Cherkasy

State University of Information and Communication Technologies, Kyiv
ORCID 0000-0003-2039-2841

Holovnia Viktoriia
Senior Lecturer of the Department of Applied Radioelectronics
Igor Sikorsky Kyiv Polytechnic Institute, Kyiv
ORCID 0000-0001-7979-1412

ONTOLOGICAL EXPERT SYSTEM FOR IDENTIFYING VULNERABLE COMPONENTS IN SECURITY SYSTEMS OF CRITICAL INFRASTRUCTURE FACILITIES

Abstract: *This paper presents an ontological expert system designed for the automated identification of vulnerable components in the security frameworks of critical infrastructure facilities. The solution is based on the use of ontologies as a formal means of knowledge representation, enabling semantic modeling of system structures, threat types, attack vectors, compromise consequences, and corresponding mitigation strategies. Unlike traditional risk analysis methods, which typically rely on fixed rules or manual interpretation, the ontological model supports logical inference of new knowledge based on the interrelationships between entities, taking into account both structural and contextual dependencies.*

The relevance of this research is driven by the complexity of modern infrastructure systems and the limitations of existing evaluation methods, which often lack scalability, fail to consider the specificity of individual objects, or do not provide interpretable results. The system's architecture includes five core modules: an OWL-based ontological knowledge base, a reasoning module using SWRL rules, a user interface for data input and visualization of results, a vulnerability and threat database (e.g., CVE, STRIDE), and a knowledge update module.

A case study was conducted using a simulated energy infrastructure object to assess the system's ability to identify complex vulnerability chains with high accuracy. System components were analyzed, outdated software and known vulnerabilities were detected, and related risks were identified with mitigation recommendations generated. Testing showed that the ontological approach outperforms traditional analysis methods in terms of accuracy, processing speed, and explainability. The results confirm the practical value of the proposed system in enhancing the cybersecurity resilience of critical infrastructure and justify the need for further research focused on integration with monitoring systems and expansion of the ontological model.

Keywords: *ontology, expert system, vulnerabilities, critical infrastructure, logical reasoning, cybersecurity.*

Постановка проблеми та її зв'язок із важливими науковими чи практичними завданнями. Сучасні об'єкти критичної інфраструктури дедалі більше залежать від складних інформаційних систем, що забезпечують управління, моніторинг і безперервне функціонування технологічних процесів [1]. Їх порушення може спричинити масштабні економічні, соціальні та екологічні наслідки, тому гарантування безпеки таких об'єктів є пріоритетним завданням національного рівня. Попри те, що системи безпеки об'єктів критичної інфраструктури включають безліч механізмів захисту, їх уразливість не є статичною величиною [2]. Вона постійно змінюється через оновлення компонентів, появу нових векторів атак, людський фактор і зміни у взаємозв'язках між підсистемами. Це ускладнює своєчасне виявлення вразливих компонентів, здатних призвести до компрометації всієї системи.

Традиційні підходи до аналізу безпеки ґрунтуються на використанні чек-листів, ручному моделюванні загроз або окремих інструментів оцінювання [3, 4]. Такі підходи не здатні повною мірою врахувати складну структуру системи, міжкомпонентні зв'язки, контекстуальні залежності та динаміку зміни стану об'єкта. У зв'язку з цим постає потреба в розробці гнучких рішень, які здатні моделювати знання про систему, загрози та її компоненти на концептуальному рівні з можливістю логічного виведення нових фактів на основі існуючих.

Одним із перспективних підходів у цьому напрямі є використання онтологічних моделей, які дозволяють формально описати структуру знань, що стосуються об'єкта критичної інфраструктури, типів його компонентів, можливих вразливостей, сценаріїв атак, а також відповідних контрзаходів. Поєднання онтологій із механізмами експертного висновку дає змогу створити експертну систему, здатну автоматизовано визначати потенційно небезпечні компоненти системи безпеки, ґрунтуючись на формалізованих знаннях і правилах.

Аналіз останніх досліджень та публікацій. Онтологічні експертні системи дедалі частіше застосовуються в галузі інформаційної безпеки для структурованого подання знань, аналізу ризиків і підтримки прийняття рішень [5]. В основі таких систем лежить формалізоване уявлення про доменну область у вигляді онтологій – семантичних моделей, які відображають сутності, їхні властивості та взаємозв'язки [6]. У контексті безпеки об'єктів критичної інфраструктури онтології дозволяють створювати гнучкі та адаптивні моделі, здатні відображати як фізичні, так і логічні компоненти

системи, потенційні загрози, способи атак, вразливості, шляхи впливу, механізми захисту.

Серед опрацьованих підходів до побудови онтологічних моделей безпеки можна виділити роботи, де розглядається застосування OWL-онтологій для моделювання вразливостей на основі баз CVE та CAPEC [7, 8]. У деяких дослідженнях пропонується створення онтологій інформаційної безпеки для визначення сценаріїв атак і вибору адекватних засобів реагування. Наприклад, розроблено онтології для опису інцидентів безпеки, типів атак, етапів компрометації систем, а також оцінки рівня ризику за методами STRIDE або DREAD [9, 10].

У публікаціях також наводяться підходи щодо побудови експертних систем, які інтегрують онтологічну модель з логічним виведенням для автоматизованого виявлення слабких місць у системі [11]. Подібні системи здатні виявляти неочевидні загрози на основі міжкомпонентних зв'язків, які важко прослідкувати в ручному режимі. Частина наукових робіт акцентує увагу на адаптивності таких систем до різних доменів, зокрема енергетики, транспортної інфраструктури, цифрових мереж.

Окрему групу становлять дослідження, присвячені комбінованим підходам, де онтологія використовується спільно з механізмами машинного навчання [12]. Це дозволяє поєднувати формальні знання з емпіричними даними, зокрема журналами подій, історіями інцидентів або результатами тестування на проникнення. Проте більшість із наявних рішень не фокусуються саме на визначенні вразливих компонентів у структурі систем безпеки об'єктів критичної інфраструктури, а розглядають безпеку на загальному рівні або лише на етапі реакції на інциденти.

Актуальним залишається завдання створення спеціалізованої онтологічної експертної системи, орієнтованої на визначення вразливих компонентів у системах безпеки об'єктів критичної інфраструктури з урахуванням типів компонентів, логіки їх взаємодії, контексту використання та потенційного впливу компрометації окремого елемента на всю систему. Така система має враховувати специфіку предметної області, забезпечувати гнучке доповнення бази знань та пояснюваність логічного виведення, що особливо важливо для експертного аналізу ризиків у відповідальних секторах.

Мета і задачі дослідження. *Метою дослідження* є розробка онтологічної експертної системи для визначення вразливих компонентів у системах безпеки об'єктів критичної інфраструктури. Завданням такої системи є не лише виявлення вразливих елементів, а й пояснення причин їхньої вразливості, аналіз залежностей між компонентами, оцінка можливого поширення впливу атаки, а також генерація рекомендацій щодо зниження ризиків. Розробка подібної системи має значну наукову і практичну цінність, оскільки сприяє підвищенню ефективності управління інформаційною безпекою в складних об'єктах та прийняттю обґрунтованих рішень в умовах обмеженого часу й ресурсів.

Виклад основного матеріалу й обґрунтування отриманих результатів дослідження. У контексті інформаційних технологій онтологія є формалізованим описом множини понять та їхніх взаємозв'язків у певній предметній області [13]. Вона визначає структуру знань у вигляді класів, об'єктів, властивостей, відношень та обмежень, забезпечуючи основу для машинного розуміння, логічного виведення та аналізу. На відміну від простих ієрархій або баз даних, онтології дозволяють не лише зберігати факти, а й інтерпретувати контекстні зв'язки між сутностями, що особливо важливо при моделюванні складних систем.

Основними властивостями онтологій є формальність, структурованість, машинна оброблюваність і можливість розширення [14]. Онтології дозволяють описувати сутності будь-якої складності, включаючи абстрактні поняття, правила поведінки систем, взаємодії між об'єктами, а також умовні залежності [15]. Завдяки цим властивостям онтології є потужним засобом подання знань у динамічних, гетерогенних середовищах.

У порівнянні з іншими методами опису знань, такими як таблиці рішень, графи залежностей чи прості XML-схеми, онтологічне моделювання забезпечує більшу гнучкість, пояснюваність і можливість логічного виведення нових фактів. Воно дозволяє не лише структурувати дані, а й автоматизовано аналізувати приховані зв'язки між компонентами системи, що робить онтології особливо корисними для виявлення слабких місць у безпекових структурах.

Онтології активно використовуються в галузях, де необхідне опрацювання знань, що швидко змінюються і мають складну структуру: у медичній інформатиці, біоінформатиці, семантичному вебі, управлінні інформаційною безпекою. Наприклад, створено онтології для опису кіберзагроз, типів вразливостей, сценаріїв атак і контрзаходів. Відомі приклади включають онтології на основі стандартів CVE, CWE, CAPEC, де знання про типи атак представлені у вигляді формалізованих схем.

Для завдань безпеки об'єктів критичної інфраструктури онтологічний підхід дає змогу врахувати типи компонентів (фізичні, програмні, мережеві), логіку їх взаємодії, потенційні вектори атак, умови активації вразливостей, а також вплив компрометації одного компонента на інші. Завдяки цьому можливо здійснювати не лише опис, а й оцінку стану системи, виявлення ризиків і підтримку

прийняття рішень.

Онтологічна експертна система, створена на основі такого підходу, включає декілька функціональних модулів, кожен з яких виконує спеціалізовану роль у процесі виявлення вразливих компонентів. Загальна архітектура такої системи подана на рис. 1.

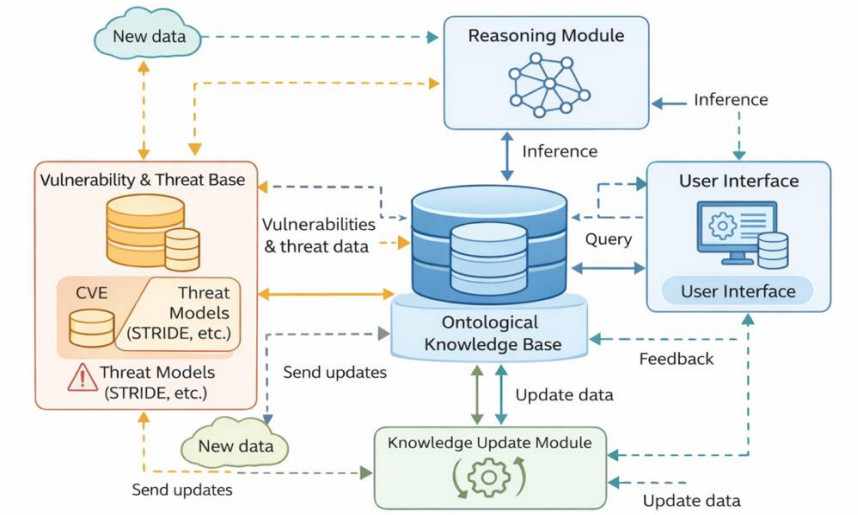

Рис. 1. Загальна архітектура онтологічної експертної системи для визначення вразливих компонентів

На схемі зображено такі основні модулі: онтологічна база знань, модуль логічного виведення, інтерфейс користувача, база типових вразливостей і загроз, модуль оновлення знань. Онтологічна база знань містить структуровану інформацію про об'єкти критичної інфраструктури, їх компоненти, функції, типові взаємозв'язки, відомі вразливості та загрози. База знань є центральною частиною системи, навколо якої організовано обчислювальні процеси.

Модуль логічного виведення реалізує правила аналізу, які дозволяють на основі комбінацій властивостей об'єктів автоматично робити висновки про їхню потенційну вразливість. Ці правила можуть включати як класичні продукційні формати, так і SWRL-записи, що застосовуються до онтологічних моделей. Інтерфейс користувача забезпечує введення даних про конкретну інфраструктуру та відображення результатів аналізу у вигляді списку вразливих компонентів з поясненням.

База вразливостей інтегрує знання з відкритих репозиторіїв (наприклад, CVE) і моделей загроз (STRIDE, MITRE ATT&CK), що дозволяє враховувати актуальні сценарії атак. Модуль оновлення забезпечує підтримку актуальності системи шляхом завантаження нових даних про загрози, а також розширення правил логічного виведення відповідно до змін у предметній області.

Взаємодія між модулями побудована так, щоб забезпечити узгоджене логічне опрацювання знань: користувач формує запит або модель об'єкта, система аналізує її відповідно до правил, використовує наявні онтологічні зв'язки та виводить перелік потенційно вразливих компонентів з відповідним рівнем ризику. Така архітектура забезпечує масштабованість, адаптивність до нових доменів і пояснюваність рішень, що є критично важливим для систем безпеки критичної інфраструктури.

У запропонованій онтологічній експертній системі знання про структуру об'єкта критичної інфраструктури, його компоненти та потенційні вразливості формалізуються у вигляді онтології, яка виступає ядром системи. Формалізація охоплює визначення основних сутностей, їхніх властивостей і зв'язків, що дозволяє здійснювати автоматизовану оцінку стану безпеки.

Ключовими сутностями є: компонент (елемент фізичної або програмної структури об'єкта), програмне забезпечення (яке встановлено на компоненті), тип атаки (наприклад, DoS, підміна даних, несанкціонований доступ), сценарій загрози (як сукупність умов, що можуть реалізувати атаку), наслідки (втрата доступності, конфіденційності, цілісності). Також виділяються поняття вразливість (як зв'язок між компонентом і потенційною атакою) та механізм захисту (наприклад, шифрування, оновлення ПЗ).

Для реалізації онтології було визначено базові класи: Component, Software, Vulnerability, Attack, ThreatScenario, Impact, Mitigation. Об'єктні властивості встановлюють відношення між класами, зокрема: hasSoftware, hasVulnerability, mayBeAttackedBy, leadsTo, hasMitigation. Дата-властивості описують числові або строкові характеристики (наприклад, версія ПЗ, дата останнього оновлення,

рівень критичності).

Фрагмент онтології, що відображає базові зв'язки між компонентами безпеки, подано на рис. 2.

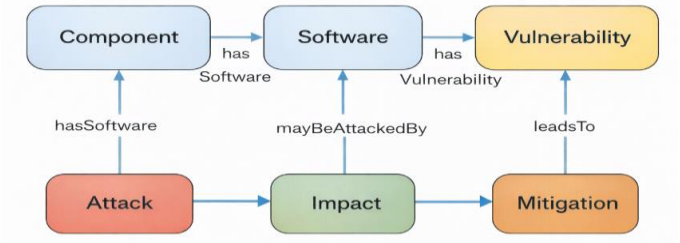

Рис. 2. Фрагмент онтології системи безпеки об'єкта критичної інфраструктури

У центрі схеми розташовано клас Component, який асоційований із Software, а той, у свою чергу, – із Vulnerability, що може бути використана для Attack. Кожна атака призводить до Impact – наприклад, зупинки функціонування, компрометації даних чи відмови системи. Для кожного типу наслідків можливе визначення доступного Mitigation.

На основі цієї структури було визначено типові шаблони вразливостей – наприклад, «Сервер → має ПЗ Apache v.2.4.51 → має вразливість CVE-2021-41773 → може бути атакований через LFI → наслідок: розкриття даних → контрзахід: оновлення до v.2.4.52».

Застосування логічного виведення в експертній системі ґрунтується на наборі правил, що формалізують залежності між властивостями сутностей. У Reasoning-модулі реалізовано правило, яке дозволяє виявити вразливий компонент на основі комбінацій його стану та виявлених ризиків. Наприклад, якщо компонент має встановлене програмне забезпечення, для якого є відкрита вразливість, і яке не оновлювалося протягом визначеного періоду, тоді виводиться твердження про високий ризик компрометації.

На рис. 3 показано типовий сценарій логічного виведення в системі, де на основі вхідних даних і правил Reasoning-модуль формує нові твердження про ризики.

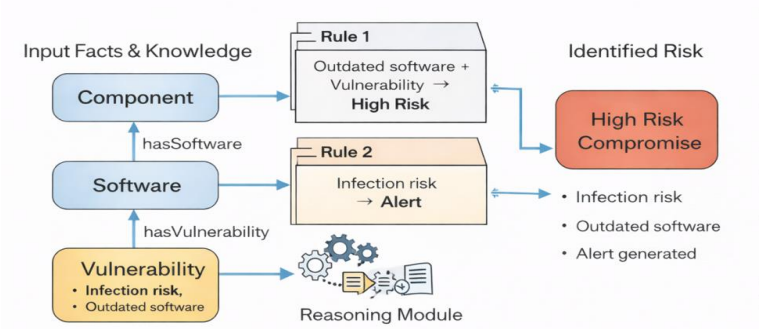

Рис. 3. Сценарій логічного виведення в онтологічній експертній системі

На схемі зображено, як з початкового факту Component → Software → Vulnerability та встановлених правил система виводить, що даний компонент піддається загрозі певного типу, та визначає рівень ризику. Ці висновки потім передаються до інтерфейсу користувача у вигляді пояснюваних результатів з посиланням на відповідні джерела та шляхи мінімізації ризику.

Для реалізації прототипу онтологічної експертної системи було використано комбінацію спеціалізованих інструментів, орієнтованих на обробку онтологій, логічне виведення та побудову користувацького інтерфейсу. Основу знань реалізовано у форматі OWL із використанням середовища Protege. Для програмного доступу до онтології застосовано OWL API (на Java) та бібліотеку RDFLib (на Python) для опрацювання RDF-графів і реалізації SPARQL-запитів. Для логічного виведення інтегровано модуль Reasoning на основі Pellet. Клієнтська частина реалізована як веб-інтерфейс на базі Flask, що забезпечує введення параметрів системи, перегляд результатів аналізу та візуалізацію вразливих компонентів.

Інтерфейс користувача дозволяє завантажити опис інфраструктури у вигляді OWL-файлу або формуляра, що заповнюється вручну. Після обробки знань Reasoning-модулем користувач отримує звіт із виявленими вразливими компонентами, їх характеристиками, ймовірним впливом і рекомендаціями щодо усунення загроз. Під час одержання (виведенні) результатів зазначається джерело знань (наприклад, CVE-ідентифікатор), логічні правила, які спрацювали, та візуалізація у вигляді графу залежностей.

Кейс-стаді було реалізовано на основі моделі енергетичного об'єкта з типовими компонентами – сервери керування, сенсорні вузли, програмно-апаратні шлюзи. Було змодельовано ситуацію, коли сервер містить застаріле ПЗ з відомою вразливістю, пов'язаною з віддаленим виконанням коду. Система вивела висновок про високий ризик компрометації та сформувала відповідні рекомендації. На рис. 4 зображено скріншот інтерфейсу з результатами запиту.

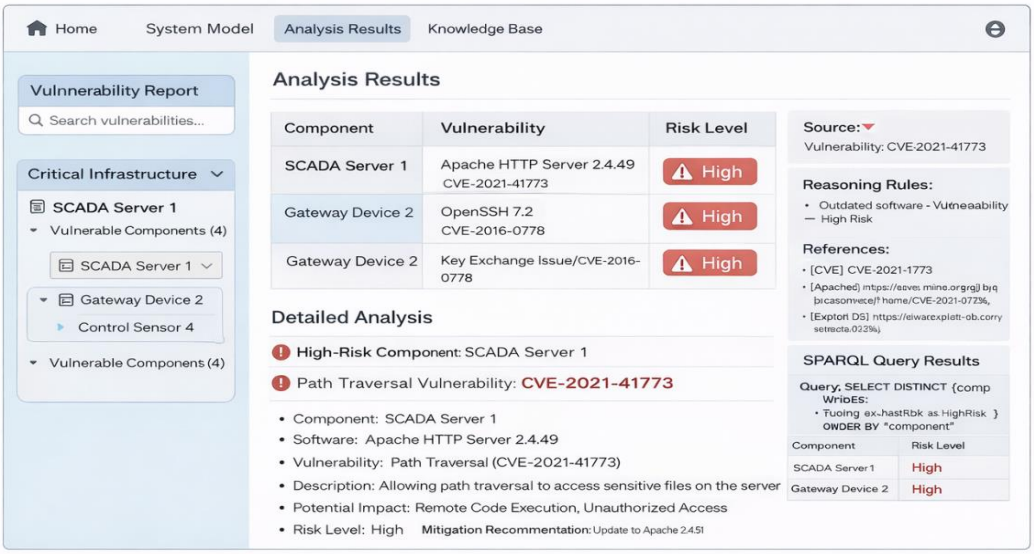

Рис. 4. Виведення результатів аналізу в інтерфейсі онтологічної експертної системи

Для оцінки ефективності системи було застосовано комбінований підхід, що включає валідацію логіки Reasoning-модуля, порівняння з ручною експертною оцінкою та тестування продуктивності. У межах експерименту змодельовано 12 типових сценаріїв, які охоплюють різні типи загроз, конфігурації інфраструктури та рівні оновлення ПЗ.

Порівняння результатів показало, що система дозволяє виявити до 92% потенційно небезпечних конфігурацій, які частково були проігноровані експертами через складність міжкомпонентних залежностей. Час виявлення вразливостей було зменшено в середньому на 47% порівняно з ручним аналізом. У табл. 1 подано порівняльні результати за основними критеріями.

Таблиця 1

Порівняльна оцінка ефективності онтологічної експертної системи та традиційного аналізу

Показник	Ручний аналіз	Онтологічна система
Точність виявлення	76%	92%
Повнота	68%	90%
Середній час оцінки (1 кейс)	18 хв	9,5 хв
Обґрунтованість результатів аналізу	Обмежена	Повна
Масштабованість на інші домени	Обмежена	Висока

Отримані результати підтверджують доцільність використання онтологічного підходу для автоматизованого виявлення вразливих компонентів і свідчать про практичну ефективність розробленої системи в умовах реальної інфраструктури.

Висновки та перспективи подальшого дослідження. У процесі дослідження було обґрунтовано доцільність використання онтологічного підходу до аналізу безпеки складних об'єктів критичної інфраструктури. Запропонована експертна система базується на формалізованому представленні знань про компоненти, їхні властивості, вразливості, атаки та наслідки, що дозволяє враховувати складні міжкомпонентні зв'язки та сценарії розвитку загроз. Побудована архітектура охоплює повний цикл обробки інформації: від введення структурованих даних до логічного виведення нових знань та візуалізації ризиків для користувача.

Розроблений прототип реалізовано з використанням сучасних інструментів опрацювання онтологій та логічного виведення. Проведене тестування показало високу точність і повноту виявлення вразливих компонентів, а також зменшення часу аналізу порівняно з ручною експертною оцінкою. Особливістю системи є можливість пояснення отриманих висновків, гнучкість у розширенні бази знань, а також адаптація до специфіки конкретного домену.

Запропонований підхід відкриває перспективи для подальшого розвитку в напрямі інтеграції з системами моніторингу подій безпеки (SIEM), автоматичного оновлення знань на основі відкритих

репозиторіїв уразливостей, а також розширення функціоналу системи для підтримки прийняття рішень у режимі реального часу. Подальші дослідження доцільно зосередити на розширенні онтологічної моделі з урахуванням динамічної поведінки компонентів, оцінці впливу суміжних ризиків і реалізації модулів прогнозування на основі логічного виведення та машинного навчання.

Внесок авторів

Інна Розломій – концептуалізація, постановка задачі дослідження, розробка методики, формування архітектури онтологічної моделі, аналіз результатів;

Віра Бабенко – наукове керівництво, валідація підходу, уточнення теоретичних положень, редагування та узгодження змісту статті;

Вікторія Головня – програмне забезпечення, реалізація онтологічної моделі та Reasoning-модуля, збір і перевірка емпіричних даних, проведення експериментального дослідження, підготовка огляду літератури.

Декларація про використання штучного інтелекту

Під час підготовки цієї статті інструменти штучного інтелекту не використовувалися. Штучний інтелект не застосовувався для отримання наукових результатів, аналізу даних, підготовки тексту, формулювання висновків або прийняття наукових рішень. Усі результати дослідження, їх інтерпретація та текст статті підготовлені авторами самостійно.

Декларація про штучний інтелект

Автор не використовував штучний інтелект при створенні матеріалів статті.

Конфлікт інтересів

Автори заявляють про відсутність конфлікту інтересів. Під час підготовки цієї роботи не існувало жодних комерційних, фінансових чи інших взаємовідносин, які могли б вплинути на результати дослідження або їх інтерпретацію. Робота виконана з дотриманням принципів академічної доброчесності, етичних норм проведення наукових досліджень і вимог редакційної політики щодо запобігання конфлікту інтересів.

Список використаної літератури

1. Barabash, O., Sobchuk, V., Musienko, A. et al. System analysis and method of ensuring functional sustainability of the information system of a critical infrastructure object. *System Analysis and Artificial Intelligence.* 2023. P. 177-192. URL: https://doi.org/10.1007/978-3-031-37450-0_11

2. Батюк, О., & Данилівський, Л. (2025). Забезпечення безпеки об'єктів критичної інфраструктури як складова національної безпеки: вітчизняний та міжнародний досвід. *Society and Security*, (6(6), 83–89. URL: https://doi.org/10.26642/sas-2024-6(6)-83-89

3. Lehto, M. Cyber-attacks against critical infrastructure. *Cyber security: Critical infrastructure protection.* 2022. P. 3-42. URL: https://doi.org/10.1007/978-3-030-91293-2_1

4. Vesić, S., Bjelajac, M. Cyber security of a critical infrastructure. *Pravo-teorija i praksa*. 2023. Vol. 40(2) P. 77-88. URL: https://www.ceeol.com/search/article-detail?id=1166617

5. Zahedi, F. M., Chen, Y., Zhao, H. Ontology-based intelligent interface personalization for protection against phishing attacks. *Information Systems Research*. 2024. Vol. 35(3). P. 1463-1478. URL: https://doi.org/10.1287/isre.2021.0065

6. Martins, B. F., Serrano Gil, L. J., Reyes Roman, J. F. et al. A framework for conceptual characterization of ontologies and its application in the cybersecurity domain. *Software and Systems Modeling*. 2022. Vol. 21(4). P. 1437-1464. URL: https://doi.org/10.1007/s10270-022-01013-0

7. Gorda, M., Levshun, D. Formalizing Knowledge on Vulnerabilities and Threats: An Ontological Approach Based on the FSTEC VDB. *International Conference on Intelligent Information Technologies for Industry*, November, 2025. P. 53-64. URL: https://doi.org/10.1007/978-3-032-13615-2_6

8. Kordi, M., Maunero, N. Ontology-driven Threat Modeling Analysis of CPSs. *CSR: 2025 IEEE International Conference on Cyber Security and Resilience,* August, 2025. P. 600-605. URL: https://doi.org/10.1109/CSR64739.2025.11129998

9. Gavric, N., Shalaginov, A., Andrushevich, A., Rumsch, A., Paice, A. Enhancing Security in International Data Spaces: A STRIDE Framework Approach. *Technologies*. 2024. Vol. 13(1). P. 8. URL: https://doi.org/10.3390/technologies13010008

10. Adach, M., Bucaioni, A., Ciccozzi, F. A Hybrid Ontology for Identifying Safety Hazards and Security Threats. *ICSRS: 2024 8th International Conference on System Reliability and Safety,* November, 2024. P. 667-676. URL: https://doi.org/10.1109/ICSRS63046.2024.10927510

11. Lupovici, A. Ontological security, cyber technology, and states' responses. *European Journal of*

International Relations. 2023. Vol. 29(1). P. 153-178. URL: https://doi.org/10.1177/1354066122113095

12. Babayeva, G., Maennel, K., Maennel, O. M. Building an ontology for cyber defence exercises. *EUROS&PW: 2022 IEEE European Symposium on Security and Privacy Workshops,* June, 2022. P. 423-432. URL: https://doi.org/10.1109/EuroSPW55150.2022.00050

13. Ayo, F. E., Awotunde, J. B., Ogundele, L. A., et al. Ontology-based layered rule-based network intrusion detection system for cybercrimes detection. *Knowledge and Information Systems*. 2024. Vol. 66(6). P. 3355-3392. URL: https://doi.org/10.1007/s10115-024-02068-9

14. Sinha, P. K., Gajbe, S. B., Debnath, S., et al. A review of data mining ontologies. *Data Technologies and Applications*. 2022. Vol. 56(2). P. 172-204. URL: https://doi.org/10.1108/DTA-04-2021-0106

15. Yang, S., Farag, M. M. G. Ontologies. *Digital Library Technologies: Complex Objects, Annotation, Ontologies, Classification, Extraction, and Security,* 2022. P. 63-88. URL: https://doi.org/10.1007/978-3-031-02285-2_3

References

1. Barabash, O., Sobchuk, V., Musienko, A. et al. System analysis and method of ensuring functional sustainability of the information system of a critical infrastructure object. *System Analysis and Artificial Intelligence.* 2023. P. 177-192. URL: https://doi.org/10.1007/978-3-031-37450-0_11

2. Batyuk, O., Danylivskyi, L. Ensuring the security of critical infrastructure facilities as a component of national security: National and international experience. *Society and Security*. 2024. Vol. 6 (6). P. 83-89. URL: https://doi.org/10.26642/sas-2024-6(6)-83-89

3. Lehto, M. Cyber-attacks against critical infrastructure. *Cyber security: Critical infrastructure protection.* 2022. P. 3-42. URL: https://doi.org/10.1007/978-3-030-91293-2_1

4. Vesić, S., Bjelajac, M. Cyber security of a critical infrastructure. *Pravo-teorija i praksa*. 2023. Vol. 40(2) P. 77-88. URL: https://www.ceeol.com/search/article-detail?id=1166617

5. Zahedi, F. M., Chen, Y., Zhao, H. Ontology-based intelligent interface personalization for protection against phishing attacks. *Information Systems Research*. 2024. Vol. 35(3). P. 1463-1478. URL: https://doi.org/10.1287/isre.2021.0065

6. Martins, B. F., Serrano Gil, L. J., Reyes Roman, J. F. et al. A framework for conceptual characterization of ontologies and its application in the cybersecurity domain. *Software and Systems Modeling*. 2022. Vol. 21(4). P. 1437-1464. URL: https://doi.org/10.1007/s10270-022-01013-0

7. Gorda, M., Levshun, D. Formalizing Knowledge on Vulnerabilities and Threats: An Ontological Approach Based on the FSTEC VDB. *International Conference on Intelligent Information Technologies for Industry*, November, 2025. P. 53-64. URL: https://doi.org/10.1007/978-3-032-13615-2_6

8. Kordi, M., Maunero, N. Ontology-driven Threat Modeling Analysis of CPSs. *CSR: 2025 IEEE International Conference on Cyber Security and Resilience,* August, 2025. P. 600-605. URL: https://doi.org/10.1109/CSR64739.2025.11129998

9. Gavric, N., Shalaginov, A., Andrushevich, A., Rumsch, A., Paice, A. Enhancing Security in International Data Spaces: A STRIDE Framework Approach. *Technologies*. 2024. Vol. 13(1). P. 8. URL: https://doi.org/10.3390/technologies13010008

10. Adach, M., Bucaioni, A., Ciccozzi, F. A Hybrid Ontology for Identifying Safety Hazards and Security Threats. *ICSRS: 2024 8th International Conference on System Reliability and Safety,* November, 2024. P. 667-676. URL: https://doi.org/10.1109/ICSRS63046.2024.10927510

11. Lupovici, A. Ontological security, cyber technology, and states' responses. *European Journal of International Relations*. 2023. Vol. 29(1). P. 153-178. URL: https://doi.org/10.1177/1354066122113095

12. Babayeva, G., Maennel, K., Maennel, O. M. Building an ontology for cyber defence exercises. *EUROS&PW: 2022 IEEE European Symposium on Security and Privacy Workshops,* June, 2022. P. 423-432. URL: https://doi.org/10.1109/EuroSPW55150.2022.00050

13. Ayo, F. E., Awotunde, J. B., Ogundele, L. A., et al. Ontology-based layered rule-based network intrusion detection system for cybercrimes detection. *Knowledge and Information Systems*. 2024. Vol. 66(6). P. 3355-3392. URL: https://doi.org/10.1007/s10115-024-02068-9

14. Sinha, P. K., Gajbe, S. B., Debnath, S., et al. A review of data mining ontologies. *Data Technologies and Applications*. 2022. Vol. 56(2). P. 172-204. URL: https://doi.org/10.1108/DTA-04-2021-0106

15. Yang, S., Farag, M. M. G. Ontologies. *Digital Library Technologies: Complex Objects, Annotation, Ontologies, Classification, Extraction, and Security,* 2022. P. 63-88. URL: https://doi.org/10.1007/978-3-031-02285-2_3

Надійшла до редакції: 08.12.25
Прийнята до друку: 17.03.26
Опубліковано: 30.03.26