УДК 004.056, 004.89 https://doi.org/10.15407/pp2025.04.078

Ю.В. Бова, О.А. Яценко

СЕМАНТИЧНИЙ ПІДХІД ДО АВТОМАТИЗОВАНОГО ФОРМУВАННЯ ДОКУМЕНТАЦІЇ СИСТЕМ БЕЗПЕКИ ІНФОРМАЦІЇ

У статті досліджується проблема автоматизованого формування складних документів для систем безпеки інформації на основі семантичного аналізу нормативно-правової бази. Проведено системний аналіз вимог нормативних документів та міжнародних стандартів щодо документування систем захисту інформації. Виявлено критичні суперечності між динамічністю нормативних вимог та статичністю існуючих інструментів автоматизації. Показано, що ручна обробка великих обсягів слабоструктурованих документів не забезпечує прийнятної якості та швидкості, а використання генеративних моделей штучного інтелекту не гарантує достовірності інформації. Обґрунтовано необхідність інтеграції засобів семантичного аналізу з інструментами генеративного штучного інтелекту для забезпечення гарантованих та пояснюваних результатів. Проаналізовано існуючі підходи до автоматизації генерації документів, включаючи шаблонні системи, засоби розмітки, онтологічні моделі та великі мовні моделі. Запропоновано концептуальну модель інтелектуальної системи підтримки авторизації безпеки інформації, що поєднує мультиагентну архітектуру, онтологічне представлення знань та можливості великих мовних моделей. Розроблено семантичний підхід до формування складних документів на основі онтологічного моделювання предметної області технічного захисту інформації. Представлена модель забезпечує трасованість між вимогами, рішеннями та джерелами знань, підтримує динамічне оновлення нормативної бази та автоматизоване формування документації відповідно до актуальних стандартів безпеки. Розроблений підхід дозволяє суттєво скоротити час та трудомісткість підготовки документації систем безпеки інформації.

Ключові слова: семантичний аналіз, онтологічне моделювання, системи безпеки інформації, автоматизована генерація документів, великі мовні моделі, нормативно-правова база, профіль безпеки, технічний захист інформації, інтелектуальні системи, формалізація знань.

Yu.V. Bova, O.A. Yatsenko

SEMANTIC APPROACH TO AUTOMATED FORMATION OF INFORMATION SECURITY SYSTEMS DOCUMENTATION

The article investigates the problem of automated generation of complex documentation for information security systems based on semantic analysis of the regulatory and legal framework. A systematic analysis of the requirements of regulatory documents and international standards for information security system documentation is conducted. Critical contradictions between the dynamic nature of regulatory requirements and the static nature of existing automation tools are identified. It is shown that manual processing of large volumes of weakly structured documents does not ensure acceptable quality and speed, while the use of generative artificial intelligence models does not guarantee the reliability of the generated information. The necessity of integrating semantic analysis tools with generative artificial intelligence to ensure guaranteed and explainable results is substantiated. Existing approaches to document generation automation are analyzed, including template-based systems, markup tools, ontological models, and large language models. A conceptual model of an intelligent information security authorization support system is proposed, combining a multi-agent architecture, ontological knowledge representation, and the capabilities of large language models. A semantic approach to the generation of complex documents based on ontological modeling of the information security engineering domain is developed. The proposed model ensures traceability between requirements, solutions, and knowledge sources, supports dynamic updates of the regulatory framework, and enables automated generation of documentation in accordance with current security standards. The developed approach significantly reduces the time and labor required for preparing information security documentation.

Keywords: semantic analysis, ontological modeling, information security systems, automated document generation, large language models, regulatory framework, security profile, technical information protection, intelligent systems, knowledge formalization.

Вступ

Документування систем безпеки інформації є критично важливим процесом, що забезпечує відповідність інформаційних систем нормативним вимогам та стандартам безпеки. Створення комплексної документації для систем захисту інформації вимагає аналізу великих обсягів нормативно-правових актів, стандартів та методичних рекомендацій, що характеризуються складною структурою, багатозначністю термінології та взаємозалежністю вимог різних рівнів.

Технічний захист інформації представляє собою приклад критичного технічного напрямку, де процеси проєктування та експлуатації інформаційних систем жорстко регламентуються нормативними документами. Предметна область характеризується високим рівнем формалізованості вимог, складною ієрархією знань та необхідністю забезпечення трасованості між вимогами, технічними рішеннями та джерелами знань.

Основним викликом у побудові інтелектуальної системи підтримки авторизації безпеки інформації є динамічність нормативно-правової бази. Зміни у вимогах безпеки, оновлення стандартів або поява нових нормативних документів вимагають постійного коригування формалізованих знань. Ручне перенесення таких змін є трудомістким процесом, схильним до помилок та суб’єктивних інтерпретацій. Крім того, нормативна документація характеризується багатозначністю термінів, складністю синтаксичних конструкцій та необхідністю забезпечення повної трасованості кожної формалізованої вимоги до її першоджерела.

Це робить критично важливим розробку методів автоматизованого отримання та формалізації вимог із слабоструктурованого тексту, що дозволить усунути ручну працю експерта, забезпечити постійну актуальність знань системи та гарантувати об'єктивність і пряму трасованість логіки до джерел.

Стан предметної області

З 2024 року в Україні активно впроваджується гармонізація національної - нормативної бази з міжнародними стандартами через застосування профілів безпеки на основі NIST SP 800-53 та NIST SP 800-171, що суттєво змінює методологію документування та авторизації систем безпеки [1].

Проведений аналіз публікацій показав, що існуючі комерційні або академічні інструментів не забезпечують комплексної підтримки оновленої нормативної бази України та повного циклу автоматизації від збору даних до генерації готових документів.

Формування профілів безпеки (ПБ) є ключовим етапом у забезпеченні інформаційної безпеки систем різного призначення. Цей процес вимагає врахування як нормативних вимог, так і специфіки об’єкта захисту, поєднуючи експертні знання із сучасними засобами автоматизації.

Виявлено критичні суперечності між динамічністю нормативних вимог та статичністю існуючих інструментів, між необхідністю повної формалізації знань та відсутністю уніфікованих машиночитаних представлень, між потребою в комплексній автоматизації та фрагментарністю наявних рішень.

На основі цього виникає потреба розробки принципово нових методів та моделей, що поєднують мультиагентну архітектуру, онтологічне представлення знань та можливості великих мовних моделей для подолання високої трудомісткості, суб'єктивності експертних оцінок та ризику помилок у підготовці пакетів документації.

Створення документації для систем безпеки інформації є багаторівневим процесом, що охоплює вимоги стандартів, моделювання, автоматизацію та оцінку ризиків.

Технології автоматизованої генерації документів. Генератори документів — це інструменти, призначені для автоматизованого створення документації на основі шаблонів та структурованих даних. До них належать як прості рішення, що

базуються на макросах Microsoft Word або VBA (Visual Basic for Applications), так і більш складні системи на основі LaTeX, Markdown, Pandoc. Ці інструменти дозволяють користувачам створювати шаблони документів із плейсхолдерами для динамічних даних, які автоматично заповнюються з баз даних, електронних таблиць.

Один із найпоширеніших підходів — це використання шаблонів у Microsoft Word [2], макросів або скриптів VBA, які заповнюють документ даними із зовнішніх джерел (наприклад, Excel або бази даних) для створення типових документів із змінними даними [3]. Цей підхід забезпечує простоту й швидкість, не потрібно вивчати спеціальні системи верстки або програмування достатньо базових знань Word. Проте така «автоматизація» не дає можливості аналізувати нормативні вимоги, структуру предметної області, логічні зв'язки між даними.

Інший підхід [4] представлений системами розмітки LaTeX або Markdown і конверторами форматів, наприклад, Pandoc. За допомогою таких систем автор формує структурований текст (з розміткою), який потім компілюється у форматовані документи (PDF, DOCX, HTML, тощо) [5]. Цей підхід дуже зручний для наукових публікацій, технічних звітів або документації, де важлива чітка структура, автоматичний зміст, покажчики, стандартизоване форматування [6]. Перевагою є розділення змісту й оформлення, автор формує «сирий» текст, а система піклується про оформлення. Це забезпечує відтворюваність, консистентність стилю, можливість автоматичного оновлення документів у разі зміни структури. Проте, як і у випадку шаблонів, ці системи не аналізують зміст документів та не дозволяють визначати семантику відношень між окремими елементами. Вони не реалізують логіку, не інтерпретують вимоги, не перевіряють відповідність даних правилам, просто відтворюють те, що їм подадуть. Для задач, де потрібно формувати документи на основі складних нормативних вимог або властивостей інформаційних систем, цього недостатньо.

Зараз активно розглядається використання LLM у синтезі документації: створення технічних специфікацій, user-guides, описів систем, де контент генерується автоматично на основі описів, кодів або структурованих метаданих. Наприклад, у недавньому дослідженні [7] показано, що поєднання LLM з онтологічним підходом дає змогу зменшити обсяг ручної роботи, підвищити стандартизацію і узгодженість документації, а також покращити її підтримку у разі зміни проєкту.

Також з'являються моделі, здатні одночасно генерувати структуру документа та його оформлення, наприклад, у роботі [8] пропонують метод autoregressive-моделювання, який враховує і текстовий вміст, і макет документа. Подібні підходи мають потенціал для створення комплексних документів з динамічним змістом і нестандартною структурою. Використання експертних систем і онтологій для автоматичного формування баз знань і правил, що лягають в основу документації з аналізу ризиків [9].

У роботі [10] розглядається застосування LLM-RAG, машинного навчання, аналітики великих даних для генерації звітів, оцінки вразливостей та підвищення якості документації.

Сучасні системи застосовують методи обробки природної мови (Natural Language Processing, NLP) і глибокі нейронні мережі для автоматичного здобуття вимог із нормативних документів, що дозволяє формувати комплаєнс-звіти та перевіряти відповідність заявлених функцій реальним можливостям пристроїв [11].

Для спрощення підтримки та оновлення знань автоматизоване формування баз знань для аналізу ризиків здійснюється шляхом трансформації елементів онтологій у правила.

Також існують спеціаізовані методи для формування профілів безпеки. Логіко-матричний метод базується на формалізації вимог нормативних документів за допомогою логічних рівнянь та матриці знань. Логіко-матричний та ймовірно-вартісний методи забезпечують високу обґрунтованість рішень, але вимагають значних часових витрат та високої квалі-

фікації експертів. Методи на основі систем підтримки ухвалення рішень та математичної оптимізації демонструють кращі показники за часом, проте є складнішими в розробці та підтримці [12].

Спільним недоліком усіх розглянутих методів є їхня ізольованість від процесу фінального документування. Вони допомагають сформувати профіль безпеки, але не забезпечують автоматичної генерації супровідної документації у стандартизованих форматах для регулятора, відсутня підтримка оновлених нормативних документів.

Аналіз літератури виявив три ключові протиріччя, що обґрунтовують необхідність розробки нових підходів.

Перше протиріччя виникає між динамічністю нормативних вимог та статичністю існуючих інструментів автоматизації. За останні роки нормативна база у сфері технічного захисту інформації зазнала фундаментальних змін, що вимагають перегляду всіх існуючих підходів до документування. Існуючі комерційні та академічні рішення не забезпечують автоматичного оновлення під час зміни нормативної бази, що призводить до швидкого застарівання їхнього функціоналу.

Друге протиріччя постає між необхідністю повної формалізації знань про предметну область та відсутністю уніфікованих машиночитаних представлень нормативних вимог. Усі розглянуті методи формування профілів захищеності базуються на експертних оцінках та вимагають ручного відображення вимог на характеристики конкретної інформаційної системи. Значна частина поданих на експертизу пакетів документації отримує негативні висновки або вимагає істотного доопрацювання, що призводить до збільшення загального терміну авторизації. Це свідчить про високу трудомісткість та суб'єктивність традиційного підходу.

Третє протиріччя виявляється між потребою в комплексній автоматизації всього циклу документування та фрагментарністю існуючих рішень. Ключовою вадою є відсутність інтегрованого підходу, що поєднував би: автоматизований збір та верифікацію даних про інформаційну систему, інтелектуальний семантичний аналіз текстів нормативних документів, автоматичну класифікацію систем на основі формалізованих правил, формування профілів безпеки відповідно до структури нормативних документів, генерацію готової документації у стандартизованих форматах.

Незважаючи на значні досягнення у застосуванні онтологічних підходів та великих мовних моделей, відсутні комплексні рішення, що поєднують гарантовану достовірність результатів семантичного аналізу з гнучкістю генеративних моделей. Існуючі методи не забезпечують повної трасованості від вихідних нормативних документів до згенерованої документації, що є критичним для систем безпеки інформації.

Мета статті полягає у розробці семантичного підходу до автоматизованого формування складних документів для систем безпеки інформації на основі онтологічного моделювання предметної області та інтеграції засобів семантичного аналізу з можливостями великих мовних моделей.

Концептуальна модель системи. Запропонована інтелектуальна система підтримки авторизації безпеки інформації базується на інтеграції трьох ключових компонентів: онтологічної бази знань, засобів семантичного аналізу та великих мовних моделей.

У процесі авторизації системи безпеки інформації (СБІ) доцільно виокремити дві основні множини документів: вхідні та вихідні. Такий поділ дозволяє формалізувати взаємозв'язок між етапами підготовки документів та спроєктувати алгоритми їхньої автоматизованої обробки.

Вхідні документи — це матеріали, які створюються на етапі проєктування інформаційної системи або надаються користувачем: опис системи, архітектура, перелік оброблюваних даних, попередні заходи безпеки. Вихідні документи — це результат роботи системи: автоматично згенеровані та перевірені звіти, профілі безпеки, що формують пакет документів для подальшого погодження.

Формально загальна множина документів може бути представлена у вигляді (1):

$$D = D_{in} \cup D_{out}. \quad (1)$$

До множини вхідних документів належать документи та дані, що формуються на етапах проєктування або експлуатації інформаційної системи (2):

$$D_{in} = \{d_1,\ d_2,\ \ldots,\ d_n\}. \quad (2)$$

Множина вихідних документів формується автоматизованою системою на основі вхідних даних та нормативної бази (3):

$$D_{out} = \{d_1,\ d_2,\ \ldots,\ d_m\}. \quad (3)$$

Таким чином, вхідні документи виступають джерелом інформації, тоді як вихідні є результатом роботи мультиагентної системи, що обробляє дані за допомогою семантичних технологій та великих мовних моделей.

Формальна модель знань

Для забезпечення уніфікованого та однозначного представлення знань предметної області пропонується онтологічна модель знань у сфері безпеки інформації (рис. 1). Вона є центральним компонентом системи та забезпечує формалізоване, структуроване представлення предметної області, виступає єдиним узгодженим джерелом знань для всіх інтелектуальних модулів системи.

Одним із важливих завдань системи є автоматизована трансформація онтологічних знань — концептів, властивостей та зв'язків — у структуровані текстові документи, що відповідають вимогам нормативно-правових актів. На відміну від традиційних підходів, де структура бази даних жорстко прив'язується до шаблонів документів, запропонований механізм ґрунтується на семантичному мапуванні, яке забезпечує гнучке та формально визначене відображення між елементами онтології та структурними компонентами цільового документа.

Нехай O — онтологія системи, а D — цільовий документ із певною структурою

$$Structure(D) = \{S_1,\ S_2,\ \ldots,\ S_n\}.$$

Семантичне мапування визначається як множина:

$$M = \{(c_i,\ s_j, f_k) : c_i \in O,\ s_j \in Structure(D), f_k \in F\}, \quad (4)$$

де c_i — концепт або властивість онтології; s_j — елемент структури документа (розділ, підрозділ, пункт); f_k — функція трансформації, що перетворює онтологічні дані у текстовий формат.

Важливою перевагою семантичного мапування є його незалежність від конкретних шаблонів документів. У разі зміни структури документа (наприклад, додавання нового розділу або пункту) достатньо лише додати нові триплети $(c_i, s_{new}, f_k) \in M$, не змінюючи саму онтологію або базу даних. Отож, онтологія виступає не лише джерелом даних, а й механізмом керованого породження текстового змісту, що гарантує семантичну відповідність інформаційної моделі нормативній структурі документа.

Використання онтологічного підходу дозволяє забезпечити семантичну узгодженість даних, підтримку логічного виведення, а також адаптивність системи до змін нормативної бази у сфері технічного захисту інформації. Застосування онтологічного підходу для формалізації знань у процесі документування систем безпеки дозволяє забезпечити цілісність нормативних вимог [13].

Ця онтологічна модель містить наступні класи:

- Normative_Document — клас нормативних документів, що регламентують вимоги до захисту інформації;

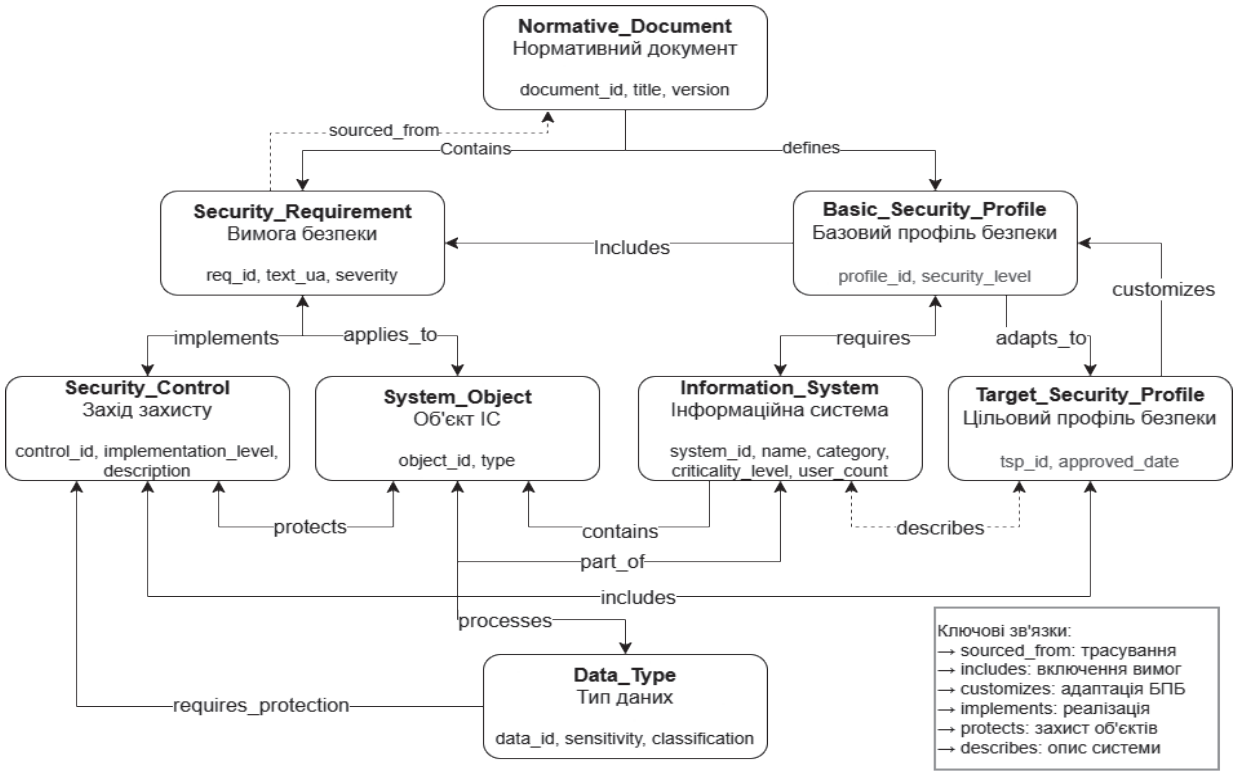

Рис. 1. Структурна схема ОМЗ

- Security_Requirement — клас вимог безпеки, сформульованих на основі нормативних документів;
- Basic_Security_Profile — клас базових профілів безпеки;
- Target_Security_Profile — клас цільових профілів безпеки, адаптованих до конкретної інформаційної системи;
- Security_Control — клас заходів захисту інформації;
- Information_System — клас інформаційних систем, для яких формується профіль безпеки;
- System_Object — клас об’єктів системи;
- Data_Type — клас типів даних, що обробляються в інформаційній системі.

Онтологічний підхід дозволяє однозначно визначити відношення між екземплярами цих класів. Виразна потужність онтології дозволяє задавати для таких відношень їхню область значення (домен) та визначення (діапазон), їхні логічні характеристики.

Наприклад, для Властивостіі s_Sourced_FromДомен — це Security_Requirement, а діапазон — Normative_Document.

В цілому структура онтології є досить стабільною — набір класів та відношень між ними змінюється дуже рідко, тільки внаслідок змін нормативних документів. Але поповнення онтології екземплярами класів на основі зовнішніх природномовних джерел знань розширює її обсяг та забезпечує акуальність представленої інформації.

Запропонована структура класів забезпечує повне покриття предметної області, дозволяє формалізувати зв’язки між нормативними вимогами, характеристиками інформаційних систем та відповідними заходами захисту.

Інтеграція з великими мовними моделями. Великі мовні моделі використовуються для розв’язання задач, що потребують розуміння контексту та генерації природномовного тексту. Зокрема, великі мовні моделі застосовуються для:

- попередньої обробки та нормалізації текстів нормативних документів;
- генерації пояснень щодо вимог безпеки та їхніх взаємозв'язків;
- формування текстових розділів документації на основі структурованих даних з онтології;
- адаптації документації до різних аудиторій та форматів представлення.

Критично важливим є забезпечення контролю достовірності генерованого контенту. Для цього використовується метод верифікації, що передбачає перевірку кожного твердження великої мовної моделі на відповідність фактам з онтологічної бази знань. Формально для кожного твердження A, згенерованого моделлю, виконується перевірка:

$$\exists T \in KB : verify(A,\ T) = true,$$

де KB — онтологічна база знань, *verify* — функція верифікації відповідності твердження триплетам онтології.

Архітектура системи формування документів. Система формування документів реалізована за мультиагентною архітектурою, що включає такі основні компоненти:

- агент аналізу нормативних документів здійснює вилучення та структурування вимог з вихідних текстів, формування онтологічних триплетів, підтримку актуальності бази знань;

- агент категоризації об'єкта захисту виконує визначення класу інформаційної системи згідно з нормативними критеріями, ідентифікацію загроз та вразливостей, оцінку рівня ризиків;

- агент формування профілю безпеки забезпечує вибір релевантних вимог та заходів захисту, формування функціонального профілю захищеності, генерацію плану імплементації заходів;

- агент генерації документації виконує формування структури документа, генерацію текстових розділів з використанням великих мовних моделей, верифікацію згенерованого контенту, форматування та експорт результатів.

Взаємодія агентів здійснюється через обмін семантичними повідомленнями, що містять онтологічні триплети та метадані про контекст виконання задачі. Це забезпечує прозорість процесу ухвалення рішень та можливість трасування кожного елемента документації до вихідних джерел.

Основні етапи обробки. У загальному випадку задача формування складних документів складається з наступних етапів.

1. Збір вхідних даних та їхнє структурування відповідно до вимог предметної області. Необхідною вимогою цього є створення структури бази знань предметної області, відповідно до якої визначаються стурктурні елементи даних (це можна розглядати як визначення набору елементів семантичної розмітки). Етап збору і обробки вхідних даних є базовим, оскільки він формує основу для подальших етапів класифікації, оцінки та генерації документації. Його основне завдання — прийняти первинні дані та документи від користувача і перетворити їх на структурований формат, зрозумілий для подальших інтелектуальних модулів системи. Цей процес є критично важливим, оскільки забезпечує перехід від неструктурованого природного тексту до формалізованого представлення знань.

2. Аналіз структрованих даних та отримання потрібної користувачу інформації, з використанням зовнішніх джерел знань та онтології предметної області, яка формалізує відношення між компонентами.

3. Перевірка відповідності семантики отриманих результатів вимогам користувача та правилам предметної області.

4. Генерація результуючого інформаційного об'єкта у формі, що відповідає правилам предметної області, та пертворення його у формат, потрібний користувачеві.

Для даної задачі ці етапи уточнюються наступним чином:

Етап 1. Отримані дані структуруються у формалізованому вигляді (JSON, RDF) і проходять процедуру семантичного мапінгу з базою знань, яка містить нормативні документи НД ТЗІ. Це дозволяє зістави-

ти характеристики інформаційної системи (ІС) із вимогами нормативної бази та виявити вади у вхідних даних. Якщо даних виявляється недостатньо, система автоматично формує запити на уточнення до користувача. Вхідними даними є базові документи, що формуються на етапі проєктування інформаційної системи, такі як концепція безпеки інформації та приватності, опис ІС, категорія критичності ІС та інші.

Етап 2. На другому етапі структуровані дані потрапляють до модуля оцінки відповідності, головним завданням якого є визначення наскільки характеристики та параметри ІС відповідають встановленим вимогам нормативних документів, здійснюється формальна класифікаці ІС, що полягає в визначеності категорії критичності.

Обробка даних відбувається за допомогою агента нормативної класифікації, який використовує онтології, що дозволяють агенту не просто шукати ключові слова, а й розуміти смислові зв'язки між різними термінами та поняттями. Це забезпечує точне та повне зіставлення вимог.

Результатом етапу є два набори даних, які стають вхідними для наступних етапів:

- перелік БПБ — базовий профіль безпеки - мінімально необхідний набір заходів і вимог, обов’язкових для ІС;
- шаблон ЦПБ — попередній проєкт цільового профілю безпеки.

Етап 3. Після класифікації здійснюється аналіз відповідності, під час якого перевіряється виконання вимог нормативних документів. Для кожного критерію визначається ступінь відповідності (повна, часткова або відсутня). Результати аналізу передаються до компонента генерації профілів, який на основі формалізованих правил формує перелік БПБ. Це забезпечує формальний перехід від характеристик ІС та нормативної бази до структурованого переліку вимог, який лягає в основу генерації кінцевих документів для авторизації.

Етап 4. Наступним етапом роботи системи є автоматизована генерація вихідних документів та формування пояснень щодо ухвалених рішень.

На вхід отримується перелік БПБ, сформований на попередньому етапі шаблон ЦПБ відповідної ІС та структуровані результати оцінки відповідності (виконані, невиконані, частково виконані вимоги). Агент генерації взаємодіє з моделлю LLM, яка не просто заповнює поля в шаблонах, а створює зв'язний та зрозумілий текст, формує пояснення . Результатом етапу є готовий ЦПБ — уніфікований документ із повним переліком заходів безпеки, а також обґрунтування, пояснення та висновки, сформовані інтелектуальною системою.

Висновки

У роботі розроблено семантичний підхід до автоматизованого формування складних документів для систем безпеки інформації, що базується на інтеграції онтологічного моделювання, семантичного аналізу та можливостей великих мовних моделей.

Запропоновано формальну модель документообігу, що розділяє вхідні та вихідні документи і дозволяє чітко визначити процес трансформації даних у готову документацію. Розроблено механізм семантичного мапування між онтологічними концептами та структурними елементами документів, що забезпечує гнучкість та незалежність від конкретних шаблонів.

Мультиагентна архітектура системи забезпечує модульність та можливість адаптації до різних предметних областей. Інтеграція великих мовних моделей під контролем онтологічної бази знань дозволяє поєднати гнучкість генерації природномовного тексту з гарантованою достовірністю інформації.

Розроблений підхід дозволяє суттєво скоротити час та трудомісткість підготовки документації систем безпеки інформації, забезпечити об’єктивність та повноту документування, підтримувати актуальність документації у разі змін нормативної бази.

Подальші дослідження будуть спрямовані на розширення онтологічної моделі для охоплення додаткових аспектів безпеки інформації, розробку методів автоматизованого виявлення неузгодженостей у нормативній базі, створення механі-

змів інтерактивної взаємодії експерта із системою для уточнення результатів, апробацію розробленого підходу на реальних проєктах систем захисту інформації. Також сферою подальших досліджень може стати застосування розобленого підходу до інших областей, де вирішення проблем потребує аналізу великих обсягів нормативних документів, обробки звітів про виконані роботи та отриманий досвід для надання рекомендацій та порад у нових обставинах з урахуванням індивідуальних особливостей користувачів. Також важливими напрямами дослідження можуть стати: аналіз виразних потужностей онтологічної моделі, можливість її масштабування та інтеграції із зовнішніми джерелами знань.

Література

1. О. В. Потій, Д. Ю. Голубничий, Ю. К. Васильєв, М. В. Єсіна, Процес декларування профілів безпеки інформації, *Радіотехніка*. 2024. № 2 (217). С. 7–22. DOI: https://doi.org/10.30837/rt.2024.2.217.01.
2. A. Javed, A. Sundrani, N. Malik, S. Prescott, Word Automation, *Robotic Process Automation using UiPath StudioX* (2021) 251-285 https://doi.org/10.1007/978-1-4842-6794-3_6.
3. Microsoft. Створення стандартизованих документів за допомогою шаблонів Word. 2025. Accessed: 28.01.2026. URL: https://learn.microsoft.com/uk-ua/power-platform/admin/using-word-templates-dynamics-365?tabs=new.
4. J. White, Using markup languages for accessible scientific, technical, and scholarly document creation, *Journal of Science Education*. 2022. Vol. 25, N 1. https://doi.org/10.14448/jsesd.14.0005.
5. D. Tenen, G. Wythoff, Sustainable authorship in plain text using Pandoc and Markdown, *The Programming Historian*. 2014. DOI: https://doi.org/10.46430/phen0041.
6. І. Сокорчук Звітна документація при освітньому процесі в дистанційній формі. Інформаційні системи та технології (ICT-2024): матеріали 13-ї Міжнар. наук.-техн. конф. С. 90–93. URL: https://ist-conf-nure.com.ua/IST-2024_part-1.pdf.
7. В. Пасічник, М. Яромич, Автоматизоване формування технічної документації в галузі іт із використанням великих мовних моделей, *Studia Methodologica*. 2025. № 59. С. 250–272.
8. S. Biswas, R. Jain, V. Morariu, J. Gu, P. Mathur, C. Wigington, T. Sun, J. Llad'os, DocSynthv2: a practical autoregressive modeling for document generation, *ArXiv*. 2024. P. 1–6. DOI: https://doi.org/10.48550/arxiv.2406.08354.
9. D. Vitkus, Z. Steckevicius, N. Goranin, D. Kalibatienė, A. Čenys, Automated expert system knowledge base development method for information security risk analysis, *International Journal of Computers Communications & Control*. 2019. Vol. 14. P. 743–758. https://doi.org/10.15837/ijccc.2019.6.3668.
10. O. A. Troian, Methods and techniques for the information and analytical systems of data protection and conversion assessment, *Ukrainian Journal of Information Technology*. 2024. Vol. 6, № 1. P. 76–85.
11. K. Ameri, M. Hempel, H. Sharif, J. Lopez, K. Perumalla, Design of a novel information system for semi-automated management of cybersecurity in industrial control systems, *ACM Transactions on Management Information Systems*. 2022. Vol. 14, N 1. P. 4–35. DOI: https://doi.org/10.1145/3546580.
12. Ostapets D., Sukhomlyn O., Analysis of existing approaches to the formation of functional security profiles, *System technologies*. 2025. Vol. 6, N 155. P. 208–217. DOI: https://doi.org/10.34185/1562-9945-6-155-2024-20.
13. Ю. В. Бова. Застосування онтологічного підходу для моделювання знань у процесі документування систем безпеки інформації. *«Безпека енергетики в епоху цифрової трансформації»: Зб.матер. сьомої науково-практичної конференції (2025, Київ)*. С. 93–95.

References

1. O. V. Potiy, D. Yu. Golubnychyy, Yu. K. Vasiliev, M. V. Yesina, The process of declaring information security profiles, in: Radiotechnics 2 (2024) 7-22. doi: 10.30837/rt.2024.2.217.01. [in Ukrainian]
2. A. Javed, A. Sundrani, N. Malik, S. Prescott, Word Automation, in: *Robotic Process Automation using UiPath StudioX* (2021). doi: 10.1007/978-1-4842-6794-3_6.
3. Microsoft. Create standardized documents using Word templates (2025). URL: https://learn.microsoft.com/uk-ua/power-

platform/admin/using-word-templates-dynamics-365?tabs=new.
4. J. White, Using markup languages for accessible scientific, technical, and scholarly document creation, in: Journal of Science Education 25 (2022). doi: 10.14448/jsesd.14.0005.
5. D. Tenen, G. Wythoff, Sustainable Authorship in Plain Text using Pandoc and Markdown, in: The Programming Historian (2014). doi: 10.46430/phen0041.
6. I. Sokorchuk, Reporting documentation in the educational process in a distance form. Information systems and technologies (IST-2024): materials of the 13th International Scientific and Technical Conference, 90-93. URL: https://ist-conf-nure.com.ua/IST-2024_part-1.pdf [in Ukrainian]
7. V. Pasichnyk, M. Yaromych, Automated generation of technical documentation in the IT industry using large language models, in: Studia Methodologica 59 (2025) 250-272. [in Ukrainian]
8. S. Biswas, R. Jain, V. Morariu, J. Gu, P. Mathur, C. Wigington, T. Sun, J. Llad'os, DocSynthv2: a practical autoregressive modeling for document generation, in: ArXiv (2024) 1-6. doi: 10.48550/arxiv.2406.08354.
9. D. Vitkus, Z. Steckevicius, N. Goranin, D. Kalibatienė, A. Čenys, Automated expert system knowledge base development method for information security risk analysis, in: International Journal of Computers Communications & Control 14 (2019) 743-758. doi:10.15837/ijccc.2019.6.3668.
10. O. A. Troian, Methods and techniques for the information and analytical systems of data protection and conversion assessment, in: Ukrainian Journal of Information Technology 6 (2024) 76-85. [in Ukrainian]
11. K. Ameri, M. Hempel, H. Sharif, J. Lopez, K. Perumalla, Design of a novel information system for semi-automated management of cybersecurity in industrial control systems, in: ACM Transactions on Management Information Systems 14 (2022) 4-35. doi:10.1145/3546580.
12. D. Ostapets, O. Sukhomlyn, Analysis of existing approaches to the formation of functional security profiles. System technologies 6 (2025) 208-217. doi: 10.34185/1562-9945-6-155-2024-20.
13. Yu. V. Bova, Application of ontological approach for knowledge modeling in the process of documenting information security systems, in: "Energy Security in the Era of Digital Transformation": Proceedings of the Seventh Scientific and Practical Conference (2025, Kyiv) 93-95. [in Ukrainian]

Одержано: 10.12.2025
Внутрішня рецензія отримана: 15.12.2025
Зовнішня рецензія отримана: 16.12.2025

Про авторів:

Бова Юрій Вікторович,
аспірант, інженер-програміст,
https://orcid.org/0009-0008-9797-5213

Яценко Олена Анатоліївна,
кандидат фізико-математичних наук,
старший науковий співробітник,
http://orcid.org/0000-0002-4700-6704

Місце роботи авторів:

[1] Інститут програмних систем
НАН України,
E-mail: bova1997@gmail.com,
oayat@ukr.net
Сайт: https://iss.nas.gov.ua