https://doi.org/10.31891/2219-9365-2026-87-40
УДК 004.056.5: 004.89

ОСТАПЕЦЬ Денис
Український державний університет науки і технологій
https://orcid.org/0000-0003-1778-7770
e-mail: odaua@i.ua
СУХОМЛИН Олексій
Український державний університет науки і технологій
https://orcid.org/0009-0006-7928-4721
e-mail: zyris21211@gmail.com

АНАЛІЗ ІНТЕЛЕКТУАЛЬНИХ МЕТОДІВ ДЛЯ ВИРІШЕННЯ ЗАДАЧІ ФОРМУВАННЯ ФУНКЦІОНАЛЬНИХ ПРОФІЛІВ ЗАХИЩЕНОСТІ ІНФОРМАЦІЇ

В роботі проведено порівняльний аналіз сучасних методів штучного інтелекту для автоматизації процесу формування функціональних профілів захищеності (ФПЗ) інформації. Розглянуто можливості застосування самоорганізуючих карт Кохонена, великих мовних моделей (LLM), експертних систем, генетичних алгоритмів та нечіткої логіки. Оцінку методів виконано за критеріями адаптивності, інтерпретованості результатів, складності реалізації та залежності від навчальних даних. Визначено ключові недоліки традиційних підходів, зокрема високий суб'єктивізм та вплив людського фактора. За результатами дослідження обґрунтовано доцільність впровадження гібридного підходу, який поєднує експертну систему як логічне ядро та LLM як інструмент інтерпретації результату, що дозволяє підвищити точність та об'єктивність проектування систем захисту.

Ключові слова: інформаційні технології, кібербезпека, інформаційна безпека, функціональний профіль захищеності інформації, штучний інтелект, експертні системи, великі мовні моделі, самоорганізуючі карти Кохонена, генетичні алгоритми, нечітка логіка.

OSTAPETS Denys, SUKHOMLYN Oleksii
Ukrainian State University of Science and Technologies

ANALYSIS OF INTELLIGENT METHODS FOR SOLVING THE PROBLEM OF FUNCTIONAL INFORMATION SECURITY PROFILES FORMATION

This paper explores the potential of applying various artificial intelligence methods to solving the problem of functional information security profile formation. Functional profiles serve as the foundational basis for secure automated systems creation, yet current formation methodologies are often hindered by subjectivity and a lack of repeatability due to heavy reliance on human expertise. The study aims to analyze intelligent means that can minimize the human factor.

The research provides a detailed comparative analysis of several key artificial intelligence technologies, including self-organizing maps, large language models, expert systems, genetic algorithms, and fuzzy logic. Each method is evaluated based on specific characteristics such as adaptability, interpretability of results, implementation complexity, and dependence on training data. Self-organizing maps are assessed for their clustering capabilities but are noted for their low interpretability. Large language models, particularly when integrated with retrieval-augmented generation, show high adaptability in providing justified recommendations based on cybersecurity standards. Expert systems are examined for their deterministic nature which ensures logical correctness, while genetic algorithms are considered for multi-objective optimization of security controls. Furthermore, fuzzy logic is highlighted for its capacity to handle uncertain linguistic variables and subjective expert assessments.

The findings indicate that while individual methods have specific strengths, no single method fully satisfies the requirements for transparency, accuracy, and regulatory compliance simultaneously. Consequently, the authors propose a hybrid conceptual approach that utilizes an expert system as the logical core to ensure strict adherence to regulatory requirements, integrated with a large language model that acts as an interpreter to transform formal rules into clear, human-readable justifications. This synergy significantly enhances the objectivity and efficiency of the information security profiling process by reducing expert bias.

Keywords: information technologies, cybersecurity, information security, functional information security profile, artificial intelligence, expert systems, large language models, Kohonen self-organizing maps, genetic algorithms, fuzzy logic.

Стаття надійшла до редакції / Received 30.06.2026
Прийнята до друку / Accepted 02.08.2026
Опубліковано / Published 10.09.2026

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Функціональні профілі захищеності інформації (ФПЗ) використовуються як база для побудови захищених автоматизованих систем у багатьох сферах діяльності. Більшість існуючих методик формування ФПЗ не можуть забезпечити повну об'єктивність та повторюваність результатів через значний вплив людського фактора. Основними недоліками традиційних підходів є їхня висока залежність від кваліфікації експерта та відсутність універсальних алгоритмів, що могли б автоматично адаптуватися до змін в інформаційній системі. Для розроблення якісного ФПЗ важливим є використання сучасних методів інтелектуального аналізу даних.

Інтелектуальні методи - це програмно-математичний інструментарій, здатний сприймати зовнішні дані, навчатися на основі досвіду та виконувати складні аналітичні функції, які раніше потребували участі людини. В представленій роботі пропонується для формування ФПЗ використовувати методи штучного інтелекту, що дозволить мінімізувати суб'єктивність експертних оцінок та підвищити точність визначення необхідного рівня протидії загрозам.

Проаналізувавши існуючі методики для рішення задачі формування ФПЗ [1], було зазначено про високий вплив кваліфікації експерта на результат сформованого ФПЗ. Задля зменшення впливу експерта, можна застосувати інтелектуальні методи.

Інтелектуальні методи знаходять своє використання у бізнесі, науці, медицині [2]. Також інтелектуальні методи доцільно використовувати в освітній галузі [3]. За допомогою інтелектуальних методів можливо оптимізувати виробничі процеси [4]. Також використання інтелектуальні методи [5] підходять для оцінки захищеності комп'ютерних систем. На зараз існує великий перелік інтелектуальних методів [6], з тих що є на зараз, для вирішення задачі формування ФПЗ, найбільш доцільно розглянути та проаналізувати наступні з них: самоорганізуючі карти Кохонена, великі мовні моделі, експертні системи, генетичні алгоритми, нечітка логіка.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Метою роботи є аналіз методів штучного інтелекту, що можуть бути використані для вирішення задачі формування ФПЗ на основі їх порівняльної характеристики. Результати роботи можуть бути використані при розробці інтелектуальних засобів автоматизованого проектування систем захисту інформації для мінімізації впливу людського фактора. Відповідно до мети в роботі поставлені такі задачі: формування вимог до характеристик методів штучного інтелекту, що можуть бути використані для формування ФПЗ, аналіз відомих інтлектуальних методів для вирішення задачі формування ФПЗ та їх порівняльна характеристика.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

У сучасному світі, штучний інтелект (ШІ) із нішевої дисципліни став базовою технологією. Якщо підсумувати терміни, що наведені у [7], штучний інтелект - це науково-технічний напрям інформатики, що охоплює теорію та практику розроблення систем, спроможних виконувати інтелектуальні (зокрема творчі) функції: сприймати й коректно інтерпретувати зовнішні дані, навчатися на основі досвіду, гнучко адаптуватися та застосовувати набуті знання для розв'язання завдань і досягнення визначених цілей.

Для порівняння методик між собою, пропонується використовувати наступні характеристики: залежність від навчальних даних, адаптивність, складність реалізації, вплив кваліфікації спеціаліста під час експлуатації, інтерпретованість результату.

Опис характеристик:

• **Залежність від навчальних даних** - характеристика, що показує наскільки методика потребує великих історичних наборів даних.

• **Адаптивність** - відображає простоту внесення змін у випадку зміни законодавства.

• **Складність реалізації** - трудомісткість розробки та налаштування методики.

• **Вплив кваліфікації спеціаліста під час експлуатації** - характеризує, якою мірою, кваліфікація експерта з ІБ, впливають на якість рішень, що отримується у результаті роботи методики.

• **Інтерпретованість результату** - характеризує, спроможність методу надати зрозуміле для людини пояснення причин вибору конкретного набору послуг безпеки.

Машинне навчання (ML). ML - це побудова моделей, що навчаються на даних. Визначають наступні способи навчання подібних моделей:

• навчання з учителем ("учитель" знає які дані необхідно отримати в результаті, та залучений у процесі навчання моделі)

• навчання без вчителя (модель сама повинна визначити залежність у вхідному векторі даних, та на виході вона повинна відповідним чином класифікувати вхідні дані)

• навчання з підкріпленням (для навчання використовується саме середовище, яке змінюється в залежності від дій моделі, причому сама модель може сприймати це середовище через набір сенсорів)

Самоорганізуючі карта Кохонена (SOM). Самоорганізована карта Кохонена - різновид нейронної мережі з навчанням без учителя. Використовується в задачах візуалізації та кластеризації. Головною особливістю SOM, що відрізняє їх від інших методів, є збереження топологічних властивостей вхідних даних. Це означає, що об'єкти (інформаційні системи, вектори загроз), які є схожими у багатовимірному просторі ознак, будуть розташовані поруч на двовимірній карті нейронів. Це дозволяє швидко й ефективно класифікувати вхідний вектор даних.

Типові задачі. Кластеризація систем/активів за ризиковими/технічними ознаками, побудова типових «портретів» для швидкого призначення шаблонів контролів.

Інструменти. Python-реалізації (MiniSom/SOMPY) або власна імплементація на JVM.

Застосування для задачі визначення ФПЗ. Вхідний вектор із параметрами середовища, вимог та обмежень проходячи через SOM, формуючи набір критеріїв захисту які у свою чергу є складовими частинами єдиного ФПЗ.

Метод самоорганізованої карти Кохонена (SOM), можна визначити такі характеристики як:

• **Залежність від навчальних даних** - висока, оскільки SOM є методом машинного навчання, для коректного формування топологічної карти та виділення стійких кластерів необхідна велика репрезентативна вибірка векторів характеристик існуючих інформаційних систем. Якість кластеризації напряму залежить від повноти та різноманітності вхідних даних.

• **Адаптивність** - низька, у випадку зміни законодавства чи нормативних вимог, сама структура навченої карти не оновлюється автоматично. Необхідно здійснити перенавчання моделі на нових даних, що вже відповідають оновленим вимогам..

• **Складність реалізації** - середня, хоча існують готові бібліотеки для реалізації алгоритму, основна трудомісткість полягає у попередній обробці та нормалізації різнорідних вхідних даних (перетворення якісних параметрів безпеки у числьові вектори) та підборі гіперпараметрів мережі (розмір решітки, швидкість навчання).

• **Вплив кваліфікації спеціаліста під час експлуатації** - середня, у штатному режимі система може автоматично відносити об'єкт до певного кластера. Проте, інтерпретація результатів для об'єктів, що потрапили на межі кластерів, вимагає від експерта глибокого розуміння контексту.

• **Інтерпретованість результату** - низька, SOM забезпечує візуальну інтерпретацію (відображає схожість систем), але не надає причинно-наслідкового пояснення вибору конкретних заходів захисту. Метод констатує факт: «Системі потрібен цей профіль, бо вона схожа на групу А», але не пояснює, чому саме, що ускладнює проходження аудиту.

Обробка природної мови (NLP) та Великі мовні моделі (LLM). Великі Мовні Моделі (Large Language Models) – це моделі машинного навчання, що використовують нейронні мережі та величезні сховища даних для вирішення завдань обробки та розуміння природної мови. Вони навчаються на великих обсягах даних, застосовують мільярди параметрів, досягаючи нового рівня якості в обробці природної мови [7].

Типові задачі. Генерація тексту/пропозицій/планів, опрацювання текстів та документації, валідація рішень, формування відповідей на основі вхідного контексу.

Інструменти. Hugging Face Transformers, LangChain, OpenAI API, LlamaIndex, spaCy.

Застосування для задачі визначення ФПЗ. Використання LLM дозволяє реалізувати підхід RAG (Retrieval-Augmented Generation). Система може здійснювати пошук по актуальній базі знань стандартів кібербезпеки та надавати експерту рекомендації щодо вибору ФПЗ, обґрунтовуючи їх посиланнями на конкретні пункти нормативних документів.

• **Залежність від навчальних даних** – висока, оскільки для функціонування LLM необхідні величезні масиви текстової інформації. Однак, у контексті прикладної задачі (RAG), акцент зміщується на якість та повноту локальної бази знань (векторного сховища), що містить нормативні документи.

• **Адаптивність** – дуже висока, при зміні законодавства чи виході нових стандартів захисту не потрібно перенавчати модель або переписувати алгоритми. Достатньо оновити контекстну базу знань, після чого система миттєво починає генерувати рекомендації з урахуванням нових вимог.

• **Складність реалізації** – середня, незважаючи на доступність готових API та бібліотек, побудова надійної архітектури RAG вимагає специфічних компетенцій у сфері інженерії запитів та налаштування векторного пошуку для мінімізації помилок генерації.

• **Вплив кваліфікації спеціаліста під час експлуатації** – висока, через імовірнісну природу генерації тексту існує ризик виникнення «галюцинацій» (хибних тверджень). Тому експерт повинен обов’язково верифікувати запропонований варіант ФПЗ.

• **Інтерпретованість результату** – висока, На відміну від класичних нейронних мереж типу «чорна скринька», архітектура RAG дозволяє супроводжувати кожну рекомендацію прямими посиланнями на релевантні пункти нормативних документів, що забезпечує верифікованість рішення. Водночас слід враховувати імовірнісну природу моделі: згенероване текстове пояснення може не повністю відображати реальний математичний ланцюжок обчислень, що призвели до цього висновку.

Експертні системи. Експертна система - це програмний засіб, що акумулює та використовує знання й досвід фахівців у конкретній предметній галузі, імітуючи міркування людини-експерта для розв’язання слабоформалізованих задач і надання консультацій менш підготовленим користувачам; на відміну від традиційних алгоритмічних процедур, такі системи спираються на знаннєві правила та евристики, а не на жорстко визначені алгоритми. Експертна система кодує знання експертів у вигляді правил («якщо/то»).

Типові задачі. Через консолідацію знань експерта, може виступати у ролі консультанта або системи прийняття рішень у будь яких сферах діяльності

Інструменти. Drools, Kogito, Jess, RuleBook, CLIPS (класичний продукційний рушій).

Застосування для задачі визначення ФПЗ: Формування ФПЗ - це «нормативна» задача з великою кількістю якщо/то залежностей. Експерт на основі свого досвіду формує базу знань яка використовується в подальшому, для визначення ФПЗ.

Метод експертних систем, можна визначити такі характеристики як:

• **Залежність від навчальних даних** – низька, оскільки в основі методу лежить не статистична обробка масивів історичних даних, а база знань, сформована на основі логічних правил та нормативних документів.

• **Адаптивність** – висока, архітектура продукційних систем дозволяє локально змінювати, додавати або видаляти окремі правила (наприклад, при оновленні версії стандарту НД ТЗІ) без порушення цілісності всієї системи та необхідності повного перенавчання.

• **Складність реалізації** – середня, основна трудомісткість полягає не в програмуванні, а в процесі наповнення бази знань — необхідності детального опитування експертів та формалізації їхнього евристичного досвіду у чіткі логічні конструкції «якщо-то».

• **Вплив кваліфікації спеціаліста під час експлуатації** – низька, система бере на себе функцію прийняття рішень, дозволяючи користувачам із меншим рівнем кваліфікації отримувати коректні рекомендації щодо ФПЗ, які відповідають рівню знань висококласного фахівця, закладеного в базу.

• **Інтерпретованість результату** – висока, механізм логічного виведення дозволяє отримати повне пояснення (traceability) прийнятого рішення, відтворивши ланцюжок спрацьованих правил. Це дає змогу чітко аргументувати вибір засобів захисту посиланням на конкретні пункти нормативних документів, що є критичним для проходження аудиту.

Генетичні алгоритми (GA). Генетичний алгоритм - це еволюційний алгоритм пошуку, що використовується для вирішення задач оптимізації і моделювання шляхом послідовного підбору, комбінування і варіації шуканих параметрів з використанням механізмів, що нагадують біологічну еволюцію.[8]

Типові задачі. Підбір конфігурацій, планування, розклад задач з обмеженнями, пошук мінімального покриття вимог за бюджетом.

Інструменти. OptaPlanner, CP-SAT (OR-Tools), ECJ.

Застосування для задачі визначення ФПЗ. Задачу доцільно формалізувати як багатокритеріальну оптимізацію з обмеженнями: за фіксованого бюджету та обов'язкових вимог до покриття вразливостей (з урахуванням імовірності та наслідків їх реалізації) потрібно відібрати комбінацію критеріїв захисту. Результатом є один або кілька Pareto-оптимальних профілів захищеності, що забезпечують максимальне ризик-орієнтоване покриття за мінімально можливих витрат і при дотриманні всіх обмежень.

Метод генетичних алгоритмів, можна визначити такі характеристики як:

• **Залежність від навчальних даних** – низька, метод не потребує накопичення великих масивів історичної статистики для навчання, оскільки базується на евристичному переборі варіантів у просторі рішень. Для роботи алгоритму достатньо наявності чітко сформульованої математичної моделі системи та функції пристосованості.

• **Адаптивність** – висока, при зміні законодавчих вимог або бюджетних обмежень достатньо скоригувати параметри цільової функції або додати нові змінні-обмеження у математичну модель, після чого алгоритм автоматично знайде нове оптимальне рішення без необхідності зміни архітектури системи.

• **Складність реалізації** – висока, головна трудність полягає у коректній математичній формалізації задачі багатокритеріальної оптимізації: визначенні ваг критеріїв, кодуванні параметрів ФПЗ у вигляді «хромосом» та налаштуванні операторів мутації/скрещування для уникнення застрягання у локальних мінімумах.

• **Вплив кваліфікації спеціаліста під час експлуатації** – низька, процес пошуку оптимального профілю відбувається автоматично за заданим алгоритмом, що мінімізує суб'єктивний фактор. Експерт впливає лише на етапі початкового налаштування моделі та ваг критеріїв.

• **Інтерпретованість результату** – середня, результатом роботи є набір Парето-оптимальних рішень, що є зрозумілим для прийняття управлінських рішень. Однак, метод не генерує лінгвістичного пояснення (логічного висновку).

Нечітка логіка (Fuzzy Logic). Нечітка логіка є математичним апаратом, що базується на узагальненні класичної логіки та теорії множин. Фундаментальна концепція цього підходу полягає у використанні функції належності, яка дозволяє елементам мати ступінь приналежності до множини в діапазоні від 0 до 1, а не обмежуватися лише бінарними значеннями («істина» або «хиба»). Це дає змогу вводити логічні операції над нечіткими множинами та оперувати лінгвістичними змінними. Завдяки такому підходу теорія нечіткої логіки дозволяє ефективно формалізувати та опрацьовувати людські знання, які зазвичай мають вигляд суб'єктивних експертних оцінок.

Нечітка логіка протиставляє чітким визначеним результатам які надаються експертними системами та оперує нечіткими лінгвістичними змінними. Процес дефазифікації - це процес переходу від нечітких лінгвістичних змін до точних результатів.

Типові задачі. Оцінювання ризиків і пріоритетів з неточними експертними судженнями; нечіткі правила управління.

Інструменти. jFuzzyLogic, FuzzyLite.

Застосування для задачі визначення ФПЗ. Переклад експертних висловлювань («критичність - висока», «загроза - середня») у числові ваги критеріїв. В результаті дефазифікації результат зводиться до сформованого ФПЗ.

Метод нечіткої логіки (Fuzzy Logic), можна визначити такі характеристики як:

• **Залежність від навчальних даних** – низька, метод не вимагає великих історичних вибірок для навчання, оскільки базується на апріорних знаннях експертів та лінгвістичних змінних.

• **Адаптивність** – середня, при зміні умов або нормативної бази (наприклад, переоцінка рівнів критичності), спеціалісту необхідно скоригувати функції належності або правила нечіткого виведення, що дозволяє гнучко налаштовувати систему під нові умови.

• **Складність реалізації** – середня, основна трудомісткість полягає у правильному визначенні лінгвістичних змінних (фазифікація) та налаштуванні правил бази знань, що вимагає глибокого розуміння предметної області для уникнення логічних суперечностей.

• **Вплив кваліфікації спеціаліста під час експлуатації** – середня, оскільки на вхід системи подаються суб'єктивні оцінки оператора (наприклад, «загроза висока»), якість кінцевого рішення залежить від адекватності цих суджень. Проте метод дозволяє нівелювати дрібні похибки та невизначеність людського сприйняття завдяки математичному апарату нечітких множин.

• **Інтерпретованість результату** – висока, логіка прийняття рішень є прозорою, оскільки оперує зрозумілими людині поняттями («ЯКЩО ризик критичний, ТО захист максимальний»). Це дозволяє надати аргументовані причини вибору конкретного ФПЗ аудиторам.

Порівняльний аналіз методів визначення ФПЗ. На основі аналізу інтелектуальних методів, виконано їх порівняння (табл. 1). Встановлено, що для задачі формування ФПЗ, яка вимагає суворої відповідності нормативним документам, критичними є інтерпретованість результату та незалежність від навчальних вибірок. Методи машинного навчання (зокрема SOM) мають ефект «чорної скриньки», що ускладнює обґрунтування рішень під час аудиту.

Найбільш доцільним є використання експертних систем, які базуються на детермінованих правилах («якщо-то»), що гарантує логічну коректність та мінімізує вплив людського фактору на результат.

Для усунення недоліку висновків у вигляді виконаних правил, пропонується гібридний підхід: використання експертної системи як логічного ядра для вибору критеріїв захисту, та інтеграція її з LLM. У такій схемі ЛЛМ не приймає рішень, а виконує роль інтерпретатора, трансформуючи спрацьовані правила у зрозумілий текстовий опис та обґрунтування для технічної документації.

Таблиця 1.

Порівняльна характеристика методів побудови ФПЗ

Метод	Залежність від навчальних даних	Адаптивність	Складність реалізації	Вплив кваліфікації спеціаліста під час експлуатації	Інтерпретованість результату
Самоорганізуючі карти Кохонена	Висока	Низька	Середня	Середній	Низька
Великі мовні моделі	Висока	Дуже висока	Середня	Високий	Висока
Експертні системи	Низька	Висока	Середня	Низький	Висока
Генетичні алгоритми	Низька	Висока	Висока	Низький	Середня
Нечітка логіка (Fuzzy Logic)	Низька	Середня	Середня	Середній	Висока

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

У процесі формування ФПЗ ключовою науково-практичною проблемою залишається високий рівень суб’єктивізму експертних оцінок, що негативно впливає на верифікованість та повторюваність результатів. Впровадження методів ШІ дозволяє перевести процес проектування ФПЗ у площину автоматизованого аналізу, де вибір критеріїв захищеності базується на об’єктивних закономірностях.

На основі проведеного порівняльного аналізу інтелектуальних методів (табл. 1) встановлено, що найбільш релевантним рішенням для вирішення поставлених задач є запропонований у роботі концептуальний підхід до створення гібридної інтелектуальної системи. В основу моделі покладено експертну систему як механізм логічного формування ФПЗ та велику мовну модель для підвищення інтерпретованості отриманого результату. Такий підхід дозволить суттєво підвищити ефективність проектування ФПЗ, мінімізуючи при цьому вплив людського фактора.

У подальшому наукового дослідження потребують питання програмної реалізації запропонованої архітектури та проведення серії експериментів для оцінки її ефективності.

Література

1. Остапець Д. О., Сухомлин О. О. Аналіз існуючих підходів до формування функціональних профілів захищеності. Системні технології. 2024. Т. 6 (155). С. 208–217. https://doi.org/10.34185/1562-9945-6-155-2024-20

2. Інформаційні технології в бізнесі. Ч. 1 : навч. посіб. / І. Б. Шевчук та ін. ; за заг. ред. І. Б. Шевчук. Львів : Видавництво ННВК «АТБ», 2020. 455 с. https://doi.org/10.32782/2524-0072/2025-72-33

3. Коломієць А., Кушнір О. Використання штучного інтелекту в освітній та науковій діяльності: можливості та виклики. Modern Information Technologies and Innovation Methodologies of Education in Professional Training Methodology Theory Experience Problems. 2023. № 70. С. 45–57. https://doi.org/10.31652/2412-1142-2023-70-45-57

4. Reyes-Perez M., Broekelmann J., Gausemeier J. Towards an Expert System for the Manufacturing System Planning of Products with Graded Properties. KEOD. 2009. P. 226–232. URL: https://pdfs.semanticscholar.org/a4b2/d494280a8292cb7097073cc43dbb7b16b17c.pdf

5. Котляров О. Ю., Бортнік Л. Л. Методи оцінки захищеності віртуальних мереж та моделі зрілості інформаційної безпеки. Computer systems and networks. 2025. Vol. 6, No. 2. P. 100-113. https://doi.org/10.23939/csn2025.02.100

6. Батареєв В. В. Методи та системи штучного інтелекту. Вісник Хмельницького національного у н

7. Юрчак І., Хіч А., Оксентюк В. Розуміння великих мовних моделей: майбутнє штучного інтелекту. Computer design systems. Theory and practice. 2024. Vol. 6, No. 2. P. 51-60. https://doi.org/10.23939/cds2024.02.051 в

8. Пиріг Я., Климаш М., Пиріг Ю., Лаврів О. Генетичний алгоритм як засіб розв'язання оптимізаційних задач. Інфокомунікаційні технології та електронна інженерія. 2023. Вип. 3, № 2, С. 95–107. https://doi.org/10.23939/ictee2023.02.095

References

pidkhodiv do formuvannia funktsionalnykh profiliv zakhyshchenosti [Analysis of existing approaches to the formation of functional security

nce in educational and scientific activities: opportunities and challenges]. Modern Information Technologies and Innovation Methodologies of

zakhyshchenosti virtualnykh merezh ta modeli zrilosti informatsiinoi bezpeky [Methods for assessing the security of virtual networks and information security maturity models]. Computer systems and networks, Vol. 6, No. 2, pp. 100–113 [in Ukrainian].

ksentiuk V. (2024) Rozuminnia velykykh movnykh modelei: maibutnie shtuchnoho intelektu [Understanding large language models: the future of artificial intelligence]. Computer design systems. Theory and practice, Vol. 6, No. 2, pp. 51–60 [in Ukrainian]. https://doi.org/10.23939/cds2024.02.051

mization problems]. Infokomunikatsiini tekhnolohii ta elektronna inzheneriia [Infocommunication technologies and electronic engineering], Vol. No. 2, pp. 95–107 [in Ukrainian]. https://doi.org/10.23939/ictee2023.02.095