

РОЗДІЛ 6

AI-ОРІЄНТОВАНА ІНЖЕНЕРІЯ ВИМОГ ДЛЯ БЕЗПЕЧНОГО ТА ЕКОЛОГІЧНОГО ПЗ

Попова Марія Олександрівна, кандидат економічних наук, доцент,
доцент кафедри інженерії програмного забезпечення, Національний
університет «Одеська політехніка», Україна, Одеса

Сучасний розвиток інформаційних технологій характеризується стрімким зростанням складності програмних систем, що обумовлює підвищення вимог до їх надійності, безпеки та ефективності використання ресурсів. У цьому контексті інженерія програмного забезпечення дедалі більше орієнтується не лише на функціональні характеристики систем, але й на нефункціональні аспекти, серед яких особливого значення набувають кібербезпека та екологічна стійкість. Врахування цих характеристик на ранніх етапах життєвого циклу програмного забезпечення, зокрема під час формування вимог, є ключовою передумовою створення якісних та надійних програмних продуктів.

Проблема полягає в тому, що традиційні підходи до інженерії вимог не забезпечують належного рівня системності при врахуванні нефункціональних характеристик. Як свідчать сучасні дослідження, значна частина помилок у програмному забезпеченні пов'язана саме з недоліками на етапі визначення вимог, зокрема з їх неповнотою, неоднозначністю або відсутністю критично важливих аспектів безпеки [1, с. 3]. Крім того, аналіз сучасних підходів показує, що вимоги до кібербезпеки часто формулюються фрагментарно та не інтегруються у загальну структуру специфікацій, що підвищує ризик виникнення вразливостей [2, с. 5].

Паралельно з цим актуалізується проблема екологічності програмного забезпечення. У сучасних дослідженнях підкреслюється, що програмні

системи мають значний вплив на енергоспоживання та використання обчислювальних ресурсів, однак питання енергоефективності рідко враховуються на етапі формування вимог [3, с. 2]. Це зумовлює необхідність інтеграції принципів сталого розвитку у процес інженерії програмного забезпечення.

Останні роки характеризуються активним впровадженням технологій штучного інтелекту у різні етапи розробки програмного забезпечення. Зокрема, використання великих мовних моделей відкриває нові можливості для аналізу текстових вимог, виявлення суперечностей та автоматичного вдосконалення специфікацій [4, с. 1]. Дослідження показують, що застосування методів обробки природної мови дозволяє підвищити якість вимог за рахунок виявлення прихованих недоліків та покращення їх узгодженості [5, с. 4].

Водночас існуючі підходи до використання штучного інтелекту в інженерії вимог переважно зосереджені на окремих аспектах аналізу тексту і не забезпечують комплексної інтеграції вимог до безпеки та екологічності. Крім того, у сучасних роботах наголошується на необхідності забезпечення прозорості та пояснюваності результатів роботи AI-систем, що є важливим фактором їх практичного застосування [6, с. 6].

Таким чином, актуальність дослідження зумовлена необхідністю розробки підходів до інженерії вимог, які поєднують можливості штучного інтелекту з принципами безпечного та екологічного проектування програмного забезпечення. Особливої ваги набуває формування таких підходів у контексті сучасних вимог до якості програмних систем та їх відповідності концепції сталого розвитку.

Метою роботи є розробка та обґрунтування підходу до AI-орієнтованої інженерії вимог, що забезпечує інтеграцію вимог кібербезпеки та енергоефективності на ранніх етапах життєвого циклу програмного забезпечення з використанням методів штучного інтелекту.

У межах проведеного дослідження було здійснено системний аналіз сучасних підходів до інженерії вимог у контексті розробки програмного забезпечення. Встановлено, що попри наявність стандартизованих процесів і методик, формування вимог залишається складною діяльністю, значною мірою залежною від людського чинника. Це пояснюється тим, що вимоги формуються в умовах взаємодії різних зацікавлених сторін, які можуть мати відмінні або навіть суперечливі очікування щодо функціональності, безпеки та ефективності системи. У результаті цього виникають неоднозначності, пропуски та логічні суперечності, які не завжди виявляються на ранніх етапах, але мають суттєвий вплив на якість кінцевого продукту.

Особливої уваги потребує питання врахування нефункціональних вимог, серед яких ключове місце займають вимоги до кібербезпеки та енергоефективності. Аналіз показав, що в більшості випадків такі вимоги або формулюються узагальнено, або залишаються поза межами специфікацій. Наприклад, вимоги до безпеки часто подаються у вигляді загальних тверджень без конкретизації механізмів їх реалізації, що ускладнює їх перевірку та впровадження. Водночас вимоги до екологічності, пов'язані з оптимізацією використання ресурсів, часто взагалі не включаються до початкових описів системи, що суперечить сучасним тенденціям сталого розвитку.

З огляду на це було запропоновано підхід до AI-орієнтованої інженерії вимог, який передбачає використання технологій штучного інтелекту як інструменту підтримки аналітика. Основна ідея полягає у поєднанні експертного досвіду людини з можливостями автоматизованого аналізу текстових даних. Такий підхід дозволяє не лише виявляти недоліки у сформульованих вимогах, але й пропонувати шляхи їх удосконалення з урахуванням сучасних вимог до безпеки та екологічності.

На початковому етапі дослідження було сформовано репрезентативний набір текстових вимог, який включає приклади з різних предметних

областей. Це дозволило врахувати різноманітність стилів формулювання та контекстів використання вимог. У процесі аналізу було встановлено, що більшість вимог мають неструктурований характер, що ускладнює їх автоматичну обробку. Для подолання цієї проблеми було застосовано семантичний підхід до аналізу тексту, який дозволяє інтерпретувати зміст вимог незалежно від їх конкретного формулювання.

Подальший етап дослідження передбачав розробку механізму виявлення прогалин у вимогах. Для цього було визначено типові характеристики безпечних та енергоефективних систем, які використовуються як орієнтири для аналізу. Інтелектуальна система здійснює порівняння наявних вимог із цими характеристиками та визначає відсутні або недостатньо деталізовані аспекти. У разі виявлення таких прогалин система формує рекомендації щодо їх уточнення, що дозволяє підвищити повноту та якість специфікації.

У процесі дослідження також було встановлено, що вимоги до безпеки та енергоефективності часто перебувають у складній взаємозалежності. Зокрема, підвищення рівня захисту може супроводжуватися зростанням обчислювального навантаження, тоді як оптимізація використання ресурсів може впливати на рівень безпеки. У зв'язку з цим запропонований підхід передбачає одночасний аналіз цих аспектів, що дозволяє знаходити збалансовані рішення та уникати односторонніх оптимізацій.

Значну увагу у дослідженні було приділено якості формулювання вимог. Було встановлено, що навіть за наявності необхідних вимог їх некоректне формулювання може призводити до помилок на наступних етапах розробки. У цьому контексті використання AI дозволяє здійснювати аналіз тексту на предмет однозначності, узгодженості та повноти. Система здатна виявляти нечіткі або двозначні формулювання та пропонувати більш точні альтернативи, що сприяє підвищенню якості документації.

Крім того, було досліджено можливість використання штучного інтелекту для узгодження вимог між різними зацікавленими сторонами. У сучасних проєктах часто виникають конфлікти між вимогами різних груп користувачів, що ускладнює процес прийняття рішень. Використання AI у цьому контексті дозволяє аналізувати такі конфлікти та пропонувати компромісні варіанти, що враховують інтереси всіх сторін.

Експериментальна апробація запропонованого підходу була проведена на прикладі розробки вебзастосунку. На першому етапі вимоги формувалися традиційним способом, після чого вони були проаналізовані з використанням AI. Отримані результати показали, що інтелектуальна система змогла виявити низку важливих аспектів, які не були враховані на початковому етапі. Зокрема, було визначено необхідність уточнення вимог до захисту даних та оптимізації використання обчислювальних ресурсів.

Подальше доопрацювання вимог із урахуванням отриманих рекомендацій дозволило підвищити їх якість, що проявилось у більшій узгодженості, деталізації та повноті. Це, у свою чергу, позитивно вплинуло на процес розробки, зменшивши кількість потенційних помилок та підвищивши ефективність взаємодії між учасниками проєкту.

Важливим аспектом дослідження стало визначення ролі аналітика у процесі AI-орієнтованої інженерії вимог. Було встановлено, що ефективність використання AI значною мірою залежить від здатності аналітика правильно інтерпретувати результати аналізу та застосовувати їх у практичній діяльності. У цьому контексті штучний інтелект виступає як інструмент підтримки прийняття рішень, а не як заміна людського досвіду.

Окрему увагу було приділено питанням прозорості та довіри до результатів роботи AI-систем. Встановлено, що для ефективного використання таких систем необхідно забезпечити можливість пояснення отриманих результатів, що дозволяє підвищити рівень довіри з боку користувачів. Це особливо важливо у сфері інженерії програмного

забезпечення, де прийняті рішення можуть мати значний вплив на безпеку та надійність систем.

У процесі дослідження було також проаналізовано вплив доменної специфіки на ефективність запропонованого підходу. Встановлено, що різні предметні області мають свої особливості, які необхідно враховувати під час аналізу вимог. Це зумовлює необхідність адаптації AI-систем до конкретного контексту використання, що підвищує точність та релевантність отриманих результатів.

Крім того, було визначено, що використання AI є особливо ефективним у великих проєктах, де кількість вимог є значною. У таких умовах автоматизація аналізу дозволяє значно скоротити час обробки інформації та зосередити увагу аналітика на більш складних завданнях, що потребують експертного втручання.

Водночас дослідження показало, що використання штучного інтелекту має певні обмеження. Зокрема, AI-системи можуть генерувати рекомендації, які потребують додаткової перевірки, оскільки вони не завжди враховують специфіку конкретного проєкту. Це підкреслює необхідність поєднання автоматизованого аналізу з експертною оцінкою.

На рисунку 1 представлено концептуальну модель результатів AI-орієнтованої інженерії вимог для безпечного та екологічного програмного забезпечення, що відображає взаємозв'язок процесів аналізу вимог, виявлення проблем і застосування штучного інтелекту з подальшим підвищенням точності вимог, рівня кібербезпеки та ефективності використання ресурсів.

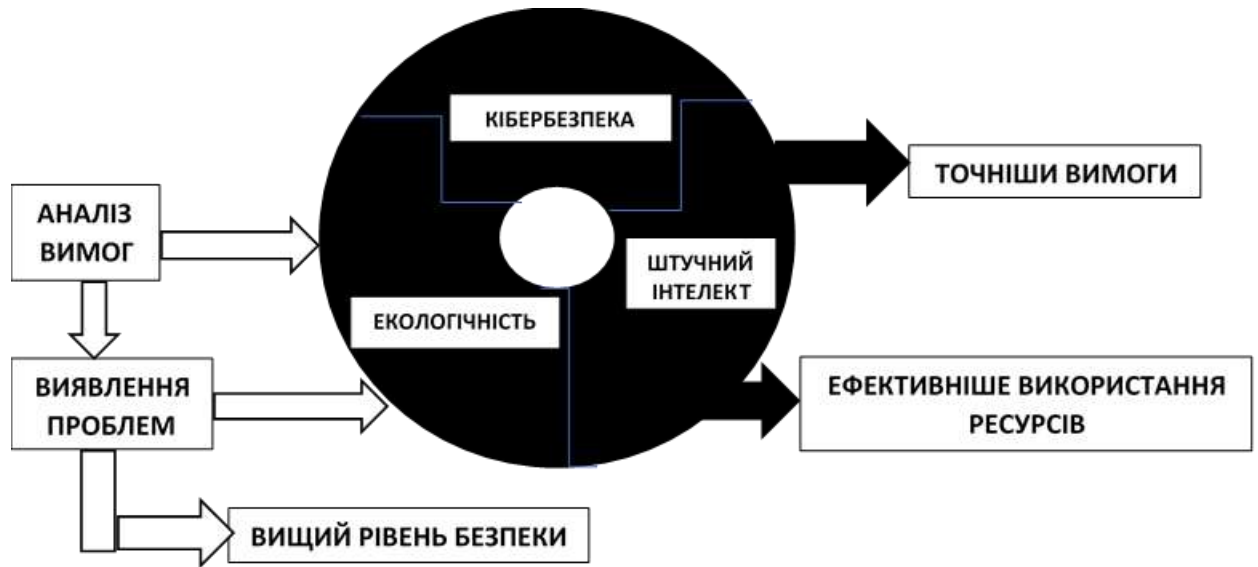


Рис. 1. Концептуальна модель результатів AI-орієнтованої інженерії вимог для безпечного та екологічного програмного забезпечення

Результати проведеного дослідження свідчать про те, що інтеграція AI у процес інженерії вимог дозволяє підвищити їх якість, забезпечити врахування важливих нефункціональних аспектів та зменшити ризик виникнення помилок на наступних етапах розробки. Такий підхід відповідає сучасним тенденціям розвитку програмної інженерії, які орієнтовані на превентивне забезпечення якості та надійності програмних систем.

Таким чином, узагальнення отриманих результатів дозволяє зробити висновок про доцільність впровадження AI-орієнтованої інженерії вимог як складової сучасних процесів розробки програмного забезпечення, що забезпечує поєднання вимог безпеки, екологічності та ефективності в єдиній узгодженій системі.

Подальший розвиток запропонованого підходу передбачає більш глибоке осмислення його місця у сучасних інженерних практиках, зокрема у контексті інтеграції з гнучкими методологіями розробки програмного забезпечення. У сучасних умовах більшість проєктів реалізується із застосуванням ітеративних та інкрементальних підходів, що передбачають

постійне уточнення та перегляд вимог. У цьому контексті використання AI-орієнтованої інженерії вимог дозволяє забезпечити безперервний аналіз та вдосконалення специфікацій, що сприяє підвищенню їх актуальності та узгодженості на кожному етапі розробки.

Зокрема, у межах гнучких методологій важливим є швидке реагування на зміни, що виникають у процесі взаємодії із замовником або користувачами. Запропонований підхід дозволяє оперативно аналізувати нові або змінені вимоги, виявляти потенційні ризики та пропонувати варіанти їх усунення. Це особливо актуально у випадках, коли зміни стосуються нефункціональних аспектів, які традиційно залишаються поза увагою або розглядаються із запізненням.

Крім того, інтеграція AI у процес інженерії вимог відкриває можливості для формування більш формалізованих і водночас гнучких моделей опису вимог. Це дозволяє поєднати переваги текстових описів із можливостями автоматизованого аналізу, що, у свою чергу, сприяє підвищенню якості комунікації між учасниками проєкту. У результаті зменшується ймовірність неправильного трактування вимог та покращується їх розуміння всіма зацікавленими сторонами.

Особливої уваги заслуговує питання використання AI для прогнозування наслідків змін у вимогах. У процесі дослідження було встановлено, що інтелектуальні системи можуть бути використані не лише для аналізу поточного стану вимог, але й для оцінювання потенційного впливу змін на інші аспекти системи. Це дозволяє приймати більш обґрунтовані рішення та уникати негативних наслідків, пов'язаних із несумісністю або конфліктами між вимогами.

У цьому контексті важливим є також забезпечення простежуваності вимог, яка є одним із ключових аспектів сучасної інженерії програмного забезпечення. Використання AI дозволяє автоматизувати процес встановлення зв'язків між різними вимогами, а також між вимогами та

іншими артефактами розробки, такими як архітектурні рішення або тестові сценарії. Це сприяє підвищенню прозорості процесу розробки та полегшує управління змінами.

Подальший аналіз показав, що застосування AI-орієнтованої інженерії вимог має позитивний вплив не лише на якість вимог, але й на загальну ефективність процесу розробки. Зокрема, було встановлено, що використання інтелектуальних інструментів дозволяє скоротити час, необхідний для аналізу та уточнення вимог, що є особливо важливим у проєктах з обмеженими ресурсами. Крім того, це сприяє зменшенню навантаження на аналітиків, дозволяючи їм зосередитися на більш складних і творчих аспектах роботи.

Водночас важливо зазначити, що впровадження запропонованого підходу потребує відповідних організаційних змін. Зокрема, необхідно забезпечити підготовку фахівців, здатних ефективно використовувати AI-інструменти у своїй діяльності. Це включає не лише технічні знання, але й розуміння принципів роботи інтелектуальних систем, а також здатність критично оцінювати отримані результати.

У процесі дослідження також було встановлено, що використання AI може сприяти формуванню нової культури роботи з вимогами, яка базується на більш високому рівні формалізації та системності. Це дозволяє підвищити рівень зрілості процесів розробки та забезпечити більш передбачувані результати. У свою чергу, це сприяє підвищенню довіри до програмних систем з боку користувачів та замовників.

Окрему увагу було приділено питанням етичного використання штучного інтелекту в інженерії вимог. Було встановлено, що при використанні AI необхідно враховувати потенційні ризики, пов'язані з упередженістю моделей або некоректною інтерпретацією даних. У зв'язку з цим важливо забезпечити контроль з боку людини, а також розробити механізми перевірки та валідації результатів роботи AI-систем.

Крім того, було визначено, що перспективним напрямом подальших досліджень є розширення можливостей AI у частині автоматичного формування вимог на основі аналізу предметної області та потреб користувачів.

Таким чином, подальший розвиток AI-орієнтованої інженерії вимог відкриває широкі можливості для вдосконалення процесів розробки програмного забезпечення. Інтеграція інтелектуальних технологій дозволяє підвищити якість вимог, забезпечити врахування критично важливих аспектів та створити умови для більш ефективного управління складними програмними системами. Це підтверджує перспективність запропонованого підходу та доцільність його подальшого дослідження і впровадження у практику.

У результаті проведеного дослідження було здійснено комплексне осмислення проблеми інженерії вимог у контексті сучасних викликів, пов'язаних із забезпеченням кібербезпеки та екологічної стійкості програмного забезпечення. Аналіз теоретичних підходів і практичних аспектів розробки програмних систем дозволив встановити, що саме етап формування вимог є критично важливим для забезпечення якості кінцевого продукту, оскільки помилки або недоліки, допущені на цьому етапі, мають тенденцію до накопичення та ускладнення на наступних стадіях життєвого циклу. У цьому контексті підтверджено, що традиційні підходи до інженерії вимог, незважаючи на їх широке використання, не повною мірою відповідають сучасним потребам, оскільки недостатньо ефективно враховують нефункціональні характеристики, зокрема вимоги до безпеки та енергоефективності.

У ході дослідження було встановлено, що однією з ключових проблем є фрагментарність і неоднозначність формулювання вимог. Значна частина специфікацій містить узагальнені або нечіткі твердження, які не забезпечують однозначного трактування та ускладнюють подальшу

реалізацію. Це особливо критично у випадку вимог до безпеки, де відсутність конкретизації може призводити до виникнення вразливостей, а також у випадку екологічних аспектів, які часто взагалі не враховуються на ранніх етапах розробки. Таким чином, підтверджено необхідність переходу від традиційних підходів до більш системних і інтелектуально підтриманих методів формування вимог.

У рамках дослідження було обґрунтовано доцільність використання технологій штучного інтелекту як інструменту підтримки процесу інженерії вимог. Визначено, що застосування AI дозволяє здійснювати глибший аналіз текстових артефактів, виявляти приховані суперечності, визначати прогалини та формувати рекомендації щодо вдосконалення вимог. При цьому важливим є те, що штучний інтелект не розглядається як автономний заміник аналітика, а виступає як допоміжний інструмент, який підсилює його професійні можливості. Такий підхід дозволяє зберегти контроль над процесом формування вимог, забезпечуючи при цьому більш високий рівень їх якості.

Особливу увагу в дослідженні було приділено інтеграції вимог до кібербезпеки та екологічності у єдину систему. Встановлено, що ці аспекти не можуть розглядатися ізольовано, оскільки вони перебувають у складній взаємозалежності. Зокрема, підвищення рівня безпеки часто супроводжується збільшенням обчислювального навантаження, що може негативно впливати на енергоефективність. Водночас надмірна оптимізація ресурсів може призводити до зниження рівня захисту. У зв'язку з цим було доведено необхідність комплексного підходу, який дозволяє знаходити збалансовані рішення з урахуванням обох аспектів.

Результати експериментальної апробації підтвердили ефективність запропонованого підходу. Зокрема, було встановлено, що використання AI дозволяє виявляти вимоги, які не були враховані на початковому етапі, а також уточнювати вже сформульовані вимоги. Це сприяє підвищенню їх

повноти, узгодженості та деталізації. У свою чергу, це позитивно впливає на процес розробки, зменшуючи кількість помилок і підвищуючи ефективність взаємодії між учасниками проєкту.

Важливим результатом дослідження є також визначення ролі аналітика у процесі AI-орієнтованої інженерії вимог. Показано, що ефективність використання AI значною мірою залежить від здатності аналітика інтерпретувати результати аналізу та приймати обґрунтовані рішення. Це свідчить про необхідність розвитку нових компетенцій у фахівців з інженерії програмного забезпечення, які повинні поєднувати знання у сфері розробки ПЗ із розумінням принципів роботи інтелектуальних систем.

Крім того, у дослідженні було розглянуто питання довіри до результатів роботи AI. Встановлено, що для широкого впровадження таких технологій необхідно забезпечити прозорість їх функціонування та можливість пояснення отриманих результатів. Це є важливою умовою прийняття рішень у сфері розробки програмного забезпечення, де помилки можуть мати значні наслідки.

Окремо було проаналізовано вплив доменної специфіки на ефективність запропонованого підходу. Встановлено, що різні предметні області мають свої особливості, які необхідно враховувати під час формування вимог. Це зумовлює необхідність адаптації AI-інструментів до конкретного контексту, що дозволяє підвищити точність аналізу та релевантність отриманих рекомендацій.

У ході дослідження також було визначено, що використання AI є особливо ефективним у великих і складних проєктах, де кількість вимог є значною. У таких умовах автоматизація аналізу дозволяє значно скоротити витрати часу та зменшити навантаження на аналітиків, що сприяє підвищенню продуктивності процесу розробки.

Разом з тим було виявлено певні обмеження запропонованого підходу. Зокрема, AI-системи можуть генерувати рекомендації, які потребують

додаткової перевірки та уточнення. Це пов'язано з тим, що такі системи працюють на основі узагальнених моделей і не завжди враховують специфіку конкретного проєкту. У зв'язку з цим підкреслено важливість поєднання автоматизованого аналізу з експертною оцінкою.

Загалом результати дослідження підтверджують, що інтеграція технологій штучного інтелекту у процес інженерії вимог є перспективним напрямом розвитку програмної інженерії. Запропонований підхід дозволяє підвищити якість вимог, забезпечити врахування важливих нефункціональних аспектів та зменшити ризик виникнення помилок. Це, у свою чергу, сприяє підвищенню надійності, безпеки та ефективності програмних систем.

Таким чином, проведене дослідження дозволяє зробити узагальнений висновок про те, що AI-орієнтована інженерія вимог є ефективним інструментом підвищення якості програмного забезпечення, який забезпечує інтеграцію вимог безпеки та екологічності у єдину узгоджену систему та відповідає сучасним тенденціям розвитку інформаційних технологій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

До розділу 1

1. Експерименти у психології: Третя хвиля Рона Джонса. URL: <https://www.psykholoh.com/post/експерименти-у-пс%25>.
2. Загадки людської психіки: Експеримент «Третя хвиля». URL: <https://revolta.com.ua/nepiznane/zagadki-lyudskoj-psihi-eksperiment-tretya-khvilya.html>.
3. Пригадуючи Третю хвилю. URL: <https://commons.com.ua/uk/prigadyuyuchi-tretyu-hvilyu/>.
4. Третя хвиля. Експеримент Рона Джонса. URL: https://psyfactor.org/lib/experiment_jonsa.htm.
5. Ghani A. Manipulation, The Third Wave Experiment. URL: <https://medium.com/illumination/manipulation-the-third-wave-experiment-a43c246e08e4>.
6. Jones Ron. Third Wave. Jones Ron. No Substitute for Madness. A Teacher, His Kids & The Lessons of Real Life. Covelo, California: Island Press, 1981. 168 p.
7. Mitchell R. The Third Wave Experiment and a Lesson from History URL: <https://www.historicmysteries.com/history/third-wave-experiment/37211/>.
8. Taaffe L. The Wave that changed the world URL: <https://www.paloaltoonline.com/news/2017/03/17/the-wave-that-changed-history/>.

To chapter 2

1. UNESCO. The Ethical Implications of the Internet of Things (IoT): Report of the World Commission on the Ethics of Scientific Knowledge and Technology (COMEST). Paris : UNESCO, 2023. 68 p. DOI: <https://doi.org/10.54678/JSGE8362>.

2. Al-Fuqaha A., Guizani M., Mohammadi M., Aledhari M., Ayyash M. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Communications Surveys & Tutorials*. 2015. Vol. 17, No. 4. P. 2347–2376. DOI: <https://doi.org/10.1109/COMST.2015.2444095>.
3. Henschke A. The Internet of Things and Dual Layers of Ethical Concern. *Robot Ethics 2.0: From Autonomous Cars to Artificial Intelligence* / ed. by P. Lin, R. Jenkins, K. Abney. New York : Oxford University Press, 2017. P. 229–243. DOI: <https://doi.org/10.1093/oso/9780190652951.003.0015>.
4. Doffman Z. Hong Kong Exposes Both Sides of China’s Relentless Facial Recognition Machine. *Forbes*. 2019. 26 August. URL: <https://www.forbes.com/sites/zakdoffman/2019/08/26/hong-kong-exposes-both-sides-of-chinas-relentless-facial-recognition-machine/> (дата звернення: 24.03.2026).
5. Taylor L., Floridi L., van der Sloot B. Introduction: A New Perspective on Privacy. *Group Privacy: New Challenges and Data Technologies* / ed. by L. Taylor, L. Floridi, B. van der Sloot. New York : Springer, 2017. P. 1–13. DOI: https://doi.org/10.1007/978-3-319-46608-8_1.
6. Slade S., Prinsloo P. Learning Analytics: Ethical Issues and Dilemmas. *American Behavioral Scientist*. 2013. Vol. 57, No. 10. P. 1510–1529. DOI: <https://doi.org/10.1177/0002764213479366>.
7. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union*. 2016. L 119. P. 1–88.
8. van den Hoven J. Fact Sheet: Ethics Subgroup IoT. Version 4.01. Brussels : European Commission, 2012. 22 p. URL: <https://www.semanticscholar.org/paper/Fact-sheet-Ethics-Subgroup-IoT->

Version-4.-0-1-Hoven/2b7d3c9f5a8e4d1f6c7b9a3e5d8f2c4a6b7e9d1f (дата звернення: 24.03.2026).

9. Fussell S. Why Can't This Soap Dispenser Identify Dark Skin? Gizmodo. 2017. 17 August. URL: <https://gizmodo.com/why-cant-this-soap-dispenser-identify-dark-skin-1797931773> (дата звернення: 24.03.2026).

10. UNESCO. "I'd Blush If I Could": Closing Gender Divides in Digital Skills through Education. Paris : UNESCO, 2019. 150 p. URL: <https://unesdoc.unesco.org/ark:/48223/pf0000367416> (дата звернення: 24.03.2026).

11. Samuel S. Alexa, Are You Making Me Sexist? Vox. 2019. 12 June. URL: <https://www.vox.com/future-perfect/2019/6/12/18660353/siri-alexa-sexism-voice-assistants-un-study> (дата звернення: 24.03.2026).

12. Brown A., Harkin D., Tanczer L.M. Safeguarding the "Internet of Things" for Victim-Survivors of Domestic and Family Violence: Anticipating Exploitative Use and Encouraging Safety-by-Design. *Violence Against Women*. 2025. Vol. 31, No. 5. P. 1039–1062. DOI: <https://doi.org/10.1177/10778012231222486>.

13. van Deursen A.J., Helsper E.J. A Nuanced Understanding of Internet Use and Non-use among the Elderly. *European Journal of Communication*. 2015. Vol. 30, No. 2. P. 171–187. DOI: <https://doi.org/10.1177/0267323115578059>.

14. Zhang K., Schnoor J.L., Zeng E.Y. E-Waste Recycling: Where Does It Go from Here? *Environmental Science & Technology*. 2012. Vol. 46, No. 20. P. 10861–10867. DOI: <https://doi.org/10.1021/es303166s>.

15. UNESCO. Report of COMEST on Land-Use Ethics. Paris : UNESCO, 2021. 52 p. URL: <https://unesdoc.unesco.org/ark:/48223/pf0000381355> (дата звернення: 24.03.2026).

16. United Nations Environment Management Group. United Nations System-wide Response to Tackling E-waste. New York : UN, 2017. 48 p.

URL: <https://unemg.org/images/emgdocs/ewaste/E-Waste-EMG-FINAL.pdf> (дата звернення: 24.03.2026).

17. Foucault M. Surveiller et punir : Naissance de la prison. Paris : Gallimard, 1975. 328 p.

18. Sassen S. Does the City Have Speech? Public Culture. 2013. Vol. 25, No. 2. P. 209–221. DOI: <https://doi.org/10.1215/08992363-2020557>.

19. Clapper J. Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community. Senate Armed Services Committee, 2016. 32 p. URL: https://www.armed-services.senate.gov/imo/media/doc/Clapper_02-09-16.pdf (дата звернення: 24.03.2026).

20. Waag Society. Making Sense: from pilots to Citizen Sensing, a Toolkit! Amsterdam : Waag Society, 2018. 36 p. URL: <https://waag.org/en/article/making-sense-pilots-citizen-sensing-toolkit> (дата звернення: 24.03.2026).

21. Gabrys J. How to Do Things with Sensors. Minneapolis : University of Minnesota Press, 2019. 106 p. DOI: <https://doi.org/10.5749/j.ctv9hj9r3>.

22. Baldini G., Botterman M., Neisse R., Tallacchini M. Ethical Design in the Internet of Things. Science and Engineering Ethics. 2018. Vol. 24, No. 3. P. 905–925. DOI: <https://doi.org/10.1007/s11948-016-9754-5>.

23. Simonite T. These Startups Are Building Tools to Keep an Eye on AI. Wired. 2019. 21 October. URL: <https://www.wired.com/story/these-startups-are-building-tools-keep-eye-ai/> (дата звернення: 24.03.2026).

24. Broadband Commission for Sustainable Development. Connecting Africa through Broadband: A Strategy for Doubling Connectivity by 2021 and Reaching Universal Access by 2030. Geneva : ITU, 2019. 48 p. URL: https://www.broadbandcommission.org/Documents/working-groups/DigitalMoonshotforAfrica_Report.pdf (дата звернення: 24.03.2026).

25. UNESCO. Recommendation on the Ethics of Artificial Intelligence. Paris : UNESCO, 2021. 48 p.

URL: <https://unesdoc.unesco.org/ark:/48223/pf0000380455> (дата звернення: 24.03.2026).

To chapter 3

1. Hutchinson T., Waters A. English for Specific Purposes: A Learning-Centred Approach. Cambridge : Cambridge University Press, 1987. 192 с.

2. Canale M., Swain M. Theoretical Bases of Communicative Approaches to Second Language Teaching and Testing. Applied Linguistics. 1980. Vol. 1, № 1. P. 1–47.

3. Гриценко Т. М. ESP-Based Sociolinguistic Exercises with AI Integration for Technical Students. Universal Teaching and Learning Journal. 2025. Vol. 1, № 3. P. 45–62. URL: <https://goodwoodpub.com/index.php/utlj/article/view/3482> (дата звернення: 21.03.2026).

4. Козлов Д., Петренко О. Enhancing ESP for STEM Students: AI Tools and Professional Communication. Tractatus. 2025. № 2. С. 17–32. URL: <https://tractatus.sumdu.edu.ua/index.php/journal/article/view/1271> (дата звернення: 21.03.2026).

5. Сидоренко І. В. Integrating Artificial Intelligence Tools into Project-Based English Language Instruction for Technical Students. Вісник Вінницького політехнічного інституту. Серія: Філософія, психологія, педагогіка. 2025. № 4. С. 78–92. URL: <http://ir.lib.vntu.edu.ua/handle/123456789/50044> (дата звернення: 21.03.2026).

6. Kozlova D., Petrenko O. AI-Enhanced Transformative Approach to ESP in Engineering Education. BCE2024 Proceedings. Tokyo : IAFOR, 2024. P. 112–125. URL: https://papers.iafor.org/wp-content/uploads/papers/bce2024/BCE2024_82559.pdf (дата звернення: 21.03.2026).

7. Alliance for Decision Education, Burning Glass Institute. Decision Skills in the Workforce: National Analysis. 2025. 45 p. URL:

<https://alliancefordecisioneducation.org/workforce-skills-report/> (дата звернення: 21.03.2026).

8. Law J. B. AI for Professional Communication : онлайн-курс. Coursera, 2026. URL: <https://www.coursera.org/learn/ai-for-professional-communication> (дата звернення: 21.03.2026).

9. UNESCO. Recommendation on the Ethics of Artificial Intelligence. Paris : UNESCO, 2021. 50 p. URL: <https://unesdoc.unesco.org/ark:/48223/pf0000381137> (дата звернення: 21.03.2026).

10. European Commission. Digital Education Action Plan (2021–2027): Reset, Progress, Challenge. Brussels : European Commission, 2025. 68 p. URL: <https://education.ec.europa.eu> (дата звернення: 21.03.2026).

11. Holmes W., Bialik M., Fadel C. Artificial Intelligence in Education: Promises and Implications for Teaching and Learning. Boston : Center for Curriculum Redesign, 2019. 128 p.

12. Godwin-Jones R. Emerging Technologies: AI and Language Learning. Language Learning & Technology. 2023. Vol. 27, № 1. P. 4–18.

До розділу 4

1. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2469-19> (дата звернення: 17.03.2026).

2. Стратегія національної безпеки України : Указ Президента України від 14.09.2020 № 392/2020. URL: <https://zakon.rada.gov.ua/laws/show/392/2020> (дата звернення: 17.03.2026).

3. Про Державну прикордонну службу України : Закон України від 03.04.2003 № 661-IV. URL: <https://zakon.rada.gov.ua/laws/show/661-15> (дата звернення: 17.03.2026).

4. Про схвалення Стратегії інтегрованого управління кордонами на період до 2025 року : розпорядження Кабінету Міністрів України від

24.07.2019 № 687-р. URL: <https://zakon.rada.gov.ua/laws/show/687-2019-p> (дата звернення: 17.03.2026).

5. Матвеев О. В. Правове регулювання прикордонної діяльності у сучасній державі : дис. ... д-ра філософії. Одеса, 2023. 238 с.

6. Конституція України : Закон України від 28.06.1996 № 254к/96-ВР. URL: <https://zakon.rada.gov.ua/laws/show/254к/96-вр> (дата звернення: 17.03.2026).

7. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19> (дата звернення: 17.03.2026).

8. Купрієнко Д. А. Основні поняття та категорії у сфері забезпечення прикордонної безпеки. Збірник наукових праць Національної академії Державної прикордонної служби України. 2014. № 1. С. 357–368.

To chapter 5

1. Про охорону праці : Закон України від 14.10.1992 р. № 2694-XII. Редакція від 01.01.2024. URL: <https://zakon.rada.gov.ua/laws/show/2694-12> (дата звернення: 19.03.2026).

2. Директива Ради 89/391/ЕЕС від 12 червня 1989 року про введення заходів для заохочення поліпшень у сфері безпеки та здоров'я працівників на роботі. Офіційний журнал Європейських Співтовариств. L 183. 29.06.1989. С. 1–8. URL: <https://www.google.com/search?q=https://eur-lex.europa.eu/legal-content/EN/TXT/%3Furi%3DCELEX:31989L0391> (дата звернення: 19.03.2026).

3. Основні шляхи реформування системи управління охороною праці в Україні - Головне управління Пенсійного фонду України в Луганській області. Головне управління Пенсійного фонду України в Луганській області. URL: <https://www.pfu.gov.ua/lg/367864-osnovni-shlyahy->

reformuvannya-systemy-upravlinnya-ohoronoyu-pratsi-v-ukrayini/ (дата звернення: 21.03.2026).

4. European Agency for Safety & Health at Work - Information, statistics, legislation and risk assessment tools. European Agency for Safety & Health at Work - Information, statistics, legislation and risk assessment tools. URL: <https://osha.europa.eu/en> (date of access: 20.03.2026).

5. ДСТУ EN ISO 45001:2019 (ISO 45001:2018, IDT). Системи управління охороною здоров'я та безпекою праці. Вимоги та настанови щодо застосування. – Київ: ДП «УкрНДНЦ», 2019.-42 с.

6. ДСТУ EN ISO 12100:2016 (EN ISO 12100:2010, IDT). Безпечність машин. Загальні принципи проєктування. Оцінювання ризиків та зменшення ризиків. Київ : ДП «УкрНДНЦ», 2016.

7. Про затвердження критеріїв, за якими оцінюється ступінь ризику від провадження господарської діяльності та визначається періодичність проведення планових заходів державного нагляду (контролю) у сфері охорони праці : Постанова Кабінету Міністрів України від 06.03.2019 р. № 223. URL: <https://zakon.rada.gov.ua/laws/show/223-2019-%D0%BF> (дата звернення: 19.03.2026).

8. Berezutskyi V. V., Samborskyi I. A. WORKPLACE SAFETY CULTURE AND RISKS OF INJURY. Labour protection problems in Ukraine. 2024. Vol. 40, no. 3-4. P. 32–41. URL: <https://doi.org/10.36804/nndipbop.40-3-4.2024.32-41> (date of access: 21.03.2026).

До розділу 6

1. Dalpiaz F., Ferrari A., Franch X. Requirements Engineering: A Roadmap. arxiv, 2022. URL: <https://arxiv.org/abs/2201.10498>

2. Nguyen D., Cruz I. Cybersecurity Requirements Engineering: A Systematic Mapping Study. IEEE Access. 2022.

3. Penzenstadler B. Sustainability in Software Engineering: Advances and Future Directions. arxiv, 2022. URL: <https://arxiv.org/abs/2206.04612>
4. OpenAI. GPT-4 Technical Report. 2023. URL: <https://arxiv.org/abs/2303.08774>
5. Ferrari A., Spagnolo G. Natural Language Processing for Requirements Engineering: Recent Trends. Requirements Engineering Journal. 2023.
6. Bommasani R. et al. On the Opportunities and Risks of Foundation Models. arxiv, 2022. URL: <https://arxiv.org/abs/2108.07258>

To chapter 7

1. Pinchuk O., Prokopenko A. Actual Areas of Development of Digital Competence of Officers of the Armed Forces of Ukraine. ICTERI 2021 Proceedings. 2021. P. 89–108. URL: https://lib.iitta.gov.ua/id/eprint/728788/1/paper_129.pdf
2. Прокопенко А. М., Пінчук О. О. Development of Digital Competence of Military Leaders in the Professional Development System. Educational Dimension. 2024. № 6. С. 112–125.
3. Нагачевський В. Я., Семів Г. О. Forming Foreign Language Communicative Competence of Future Ukrainian Armed Forces Officers by Means of ICT. Online Defense. 2024. Vol. 45, № 2. P. 78–92.
4. Professional Military Education Modernization and CGSC Transformation. Small Wars Journal. 2025. URL: <https://smallwarsjournal.com/2025/10/29/pme-modernization-cgsc-transformation/> (дата звернення: 21.03.2026).
5. Nahachevskiy V. Yo., Semiv G. O. Information and Communication Technologies in the Formation of Professional Competence of Cadets of Ukrainian Military Higher Educational Institutions during Wartime. Prospects and Innovations of Science. Series Pedagogy. 2025. No. 10(56). P. 74–87.
6. Professional Military Education Modernization and CGSC Transformation. Small Wars Journal. 2025.

7. NATO StratCom COE. Digital Competence Framework for Military Professionals. Riga : NATO StratCom COE, 2024. 72 с.
8. NATO. Allied and Joint Approaches to Digital Transformation and Multi-Domain Operations. 2022–2024.
9. U.S. Army. Army Learning Concept for 2030–2040. Washington : TRADOC, 2023. 45 с.
10. NATO. Interoperability, Strategic Communication, and Military Professional Development Documents. Brussels : NATO, 2024.
11. European Commission. Digital Competence Framework for Citizens (DigComp 2.2). Brussels : EC, 2022. URL: https://joint-research-centre.ec.europa.eu/digcomp_en (дата звернення: 21.03.2026)
12. Бахмат Н. В. Цифрова трансформація військової освіти України. Військова освіта. 2025. № 1. С. 5–20.
13. Rodikov V. Interdisciplinary Professional Training of Military Specialists. Advances in Military Education. 2025. Vol. 3, No. 1. P. 23–38.

To chapter 8

1. Ouyang Z. et al. Self-regulated learning and engagement as serial mediators between AI-driven adaptive learning platform characteristics and educational quality. *Frontiers in Psychology*. 2025. Vol. 16. Article 1646469. DOI: 10.3389/fpsyg.2025.1646469.
2. Liu G. L. A scoping review of AI-mediated informal language learning: Mapping out the territory. *ReCALL*. 2026. Vol. 38, № 1. P. 1–25.
3. Järvelä S., Hadwin A. F. Self-regulation and shared regulation in collaborative learning in adaptive digital learning environments. *British Journal of Educational Technology*. 2024. Vol. 55, № 5. P. 1892–1915.
4. Huang Y. et al. L2 growth mindset in AI-mediated language learning: The mediating roles of emotional intelligence and willingness to

communicate. *Frontiers in Psychology*. 2025. Vol. 16. Article 1700117. DOI: 10.3389/fpsyg.2025.1700117.

5. Dovhaniuk E. Multimodal and cognitive approaches to academic discourse in AI-integrated learning environments. *Cognition, Communication, Discourse*. 2025. № 24. P. 15–32.

6. Winne P. H., Hadwin A. F. Studying as self-regulated learning. *Metacognition in Educational Theory and Practice* / ed. by D. J. Hacker, J. Dunlosky, A. C. Graesser. Mahwah : Lawrence Erlbaum Associates, 1998. P. 277–304.

To chapter 9

1. Бахмат Н. В. Штучний інтелект у вищій освіті: можливості, виклики, перспективи. *Педагогічні науки: теорія, історія, інноваційні технології*. 2023. № 3. С. 12–25.

2. Алексеєва Г. М. Етичні та освітні виклики штучного інтелекту у вищій освіті України. Науково-дослідна робота в системі підготовки фахівців-педагогів : матер. X Всеукр. наук.-практ. конф. Запоріжжя : БДПУ, 2025. С. 9–12.

3. Козлов Д. А. Використання штучного інтелекту у вищій освіті: стан і перспективи. *International Scientific Journal of Elementary and Secondary Education*. 2024. № 1. С. 45–58.

4. Holmes W., Bialik M., Fadel C. *Artificial Intelligence in Education: Promises and Implications for Teaching and Learning*. Boston : Center for Curriculum Redesign, 2019. 128 p.

5. UNESCO. *Recommendation on the Ethics of Artificial Intelligence*. Paris : UNESCO, 2021. 50 p. URL: <https://unesdoc.unesco.org/ark:/48223/pf0000381137>

6. European Network for Academic Integrity. *Guidelines on Ethical Use of AI in Education*. 2025.

7. Shaw A. et al. Student Willingness to Use Generative AI Despite Policy Prohibitions. *Journal of Academic Ethics*. 2023. Vol. 21, No. 4. P. 567–589.

8. Godwin-Jones R. Emerging Technologies: AI and Language Learning. *Language Learning & Technology*. 2023. Vol. 27, No. 1. P. 4–18.

9. Akgun S., Greenhow C. Artificial Intelligence in Education: Addressing Ethical Challenges in K-12 Settings. *AI and Ethics*. 2022. Vol. 2, No. 3. P. 431–440.

10. Hutchinson T., Waters A. *English for Specific Purposes: A Learning-Centred Approach*. Cambridge : Cambridge University Press, 1987. 192 p.

11. Canale M., Swain M. Theoretical Bases of Communicative Approaches to Second Language Teaching and Testing. *Applied Linguistics*. 1980. Vol. 1, No. 1. P. 1–47.

12. European Commission. *Digital Education Action Plan (2021–2027): Reset, Progress, Challenge*. Brussels : European Commission, 2025.

До розділу 10

1. Акмеологія: методологічні принципи і підходи [Електронний ресурс]. Освіта.уа. Режим доступу: <https://osvita.ua/vnz/reports/sociology/29809/>.

2. Боднар А. Л. Самореалізація творчого потенціалу людини в акмеології: науково-методологічні орієнтації. Київ, 2017. 180 с.

3. Войнікова А., Бетехтін О. Акмеологічний підхід у професійному розвитку майбутніх керівників освітніх закладів. *Педагогічний журнал*. 2025. № 1–2. С. 45–52.

4. Дубасенюк О. А. Методологія впровадження акмеологічного підходу у професійній підготовці педагога. Текст електронного ресурсу. Запорізький нац. ун-т, 2024. Режим доступу: <http://eprints.zu.edu.ua/>

5. Огнев'юк В. О. Сучасні акмеологічні дослідження: теоретико-методологічні та прикладні аспекти / В. О. Огнев'юк, С. О. Сисоєва, Я. С. Фруктова (ред.). Київ : Київський ун-т ім. Б. Грінченка, 2016. 200 с.
6. Паламарюк В. А. Формування акмеологічної компетентності педагога: теоретико-методологічні підходи. Одеса, 2025. 210 с.
7. Саяпіна С. А. Акмеологічні технології: методичні вказівки. Дніпро : ДДПУ, 2020. 32 с.
8. Саяпіна С. А. Акмеологічні технології: три методологічні орієнтації сучасного знання (природничо-наукова, гуманітарна, технологічна). Дніпро, 2021. 120 с.
9. Сучасні акмеологічні дослідження: теоретико-методологічні та прикладні аспекти : зб. наук. пр. / [ред. кол. В. О. Огнев'юк та ін.]. Київ : Київський ун-т ім. Б. Грінченка, 2016–2025. Серія: Акмеологія. Вип. 1–10.

Vydavatel:

Publishing house Education and Science s.r.o. IČO : 271 56 877.
Frýdlanská 15/1314 , Praha 8. MS v Praze , oddíl C, vložka 100614

**Cross-Disciplinary Studies in
Science, Innovation and Social
Development**

Volume VIII

Signed for printing on March 28, 2026.
Format 60x90/8. Headset Times New Roman.
Mental printing. arc. 5,04. Edition online.