УДК 004.8:004.056

Л. М. Куперштейн, канд. техн. наук, доц.; В. В. Волинець;
О. П. Войтович, канд. техн. наук, доц.

АНАЛІЗ СУЧАСНИХ ПІДХОДІВ ТА ПЕРСПЕКТИВ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В АУДИТІ КІБЕРБЕЗПЕКИ ПІДПРИЄМСТВА

У роботі досліджено сучасні підходи до застосування штучного інтелекту в аудиті кібербезпеки підприємства та обґрунтовано доцільність їх використання для підвищення ефективності аудиторських процедур у динамічному середовищі кіберзагроз. Актуальність теми зумовлена тим, що традиційний аудит спирається на ручний збір доказів, періодичні перевірки та постфактум-аналіз, що ускладнює своєчасне виявлення інцидентів і підвищує ризик пропуску критичних відхилень. Метою статті є аналіз можливостей застосування систем на основі правил, методів машинного та глибокого навчання, великих мовних моделей і автономних агентів для автоматизації збору доказів, виявлення аномалій, оцінювання ризиків, перевірки відповідності вимогам стандартів і підготовки звітності. У статті узагальнено базові етапи процесу аудиту кібербезпеки та показано, на яких етапах інтелектуальні технології здатні забезпечити найбільший ефект. Проведено порівняльний аналіз підходів штучного інтелекту за критеріями точності, адаптивності, пояснюваності, ризику хибних спрацювань і придатності до типових аудиторських завдань. Показано, що системи на основі правил доцільні для контролю відповідності, тоді як моделі машинного навчання ефективні для оцінювання ризиків і класифікації подій, а методи навчання без учителя та гібридні архітектури мають високий потенціал для виявлення аномалій. Окрему увагу приділено використанню генеративного штучного інтелекту для аналізу нормативної документації, формування чернеток звітів і створення синтетичних даних. Встановлено, що найбільш перспективними є гібридні рішення, які поєднують прозорість експертних правил з адаптивністю моделей навчання. Водночас визначено ключові обмеження впровадження штучного інтелекту: галюцинації, залежність від якості даних, потребу в пояснюваності рішень та необхідність захисту інтелектуальних агентів.

Ключові слова: *штучний інтелект, машинне навчання, кібербезпека, аудит безпеки підприємства, автоматизація аудиту, виявлення аномалій, кіберзагроза, вразливість.*

Вступ

В умовах стрімкої цифровізації та зростання кіберзагроз аудит кібербезпеки стає критичним елементом забезпечення стійкості організацій. Відповідно до міжнародних стандартів, зокрема ISO 19011, аудит визначається як систематичний, незалежний і документований процес отримання об'єктивних доказів та їх об'єктивного оцінювання для визначення ступеня виконання критеріїв аудиту [1]. Цей процес є комплексним і складається з трьох основних компонентів: адміністративних (політики безпеки, управління ризиками), технічних (автентифікація, шифрування, контроль доступу, аналіз вразливостей) та фізичних (захист периметра, відеоспостереження) [2].

Проведення аудиту сьогодні є надзвичайно складним та ресурсомістким завданням. Головна складність полягає у тому, що традиційні методології значною мірою покладаються на ручну працю, яка погано масштабується в сучасних гетерогенних середовищах. Найбільш ресурсомістким етапом є збір доказів. Аудитори змушені вручну збирати скріншоти конфігурацій, вивантажувати логи з сотень систем та заповнювати незліченні таблиці, що значно знижує ефективність процесу через його трудомісткість та високу ймовірність механічних помилок [3]. Дослідження показують, що ручний збір доказів є повільним, дорогим і часто призводить до отримання застарілих даних ще до моменту завершення звіту [4]. Іншим часомістким аспектом є аналіз журналів подій та моніторинг активності. Дослідження підтверджують, що для ефективної протидії сучасним векторам атак аудитори повинні переходити від періодичних перевірок до безперервного моніторингу з використанням автоматизованих засобів, оскільки покладання виключно на ручні методи

підвищує ризик пропуску критичних інцидентів [5].

Проблема, що розглядається у цій статті, полягає у розриві між динамікою розвитку кіберзагроз та статичністю традиційних методів аудиту. Наявні підходи, засновані на періодичних перевірках та ручній обробці даних, є реактивними і не дозволяють отримувати об'єктивну картину стану безпеки в режимі реального часу. Ручні методи аудиту характеризуються високою трудомісткістю, суб'єктивністю оцінок та нездатністю обробляти великі обсяги даних, що створює "сліпі зони" в системі захисту та підвищує ризики успішних кібератак [3].

Метою статті є дослідження доцільності використання методів штучного інтелекту (ШІ), зокрема, класичного машинного навчання, глибоких нейромереж та великих мовних моделей для автоматизації процесів аудиту кібербезпеки. Тому необхідно проаналізувати ефективність застосування ШІ для вирішення специфічних аудиторських задач (таких як збір доказів, виявлення аномалій, генерація звітів) та систематизувати сфери їх застосування, виокремивши переваги та обмеження кожного підходу.

Результати дослідження

Для розуміння трансформаційного впливу ШІ необхідно спершу формалізувати базовий процес аудиту. Відповідно до стандартів серії ISO/IEC 27000 та настанов ISO 19011, процес аудиту інформаційної безпеки є циклічним і складається з таких ключових етапів: ініціювання та планування, попередній огляд документації, збір аудиторських доказів (польовий етап), аналіз та оцінка невідповідностей, і, нарешті, звітування (рис. 1) [1].

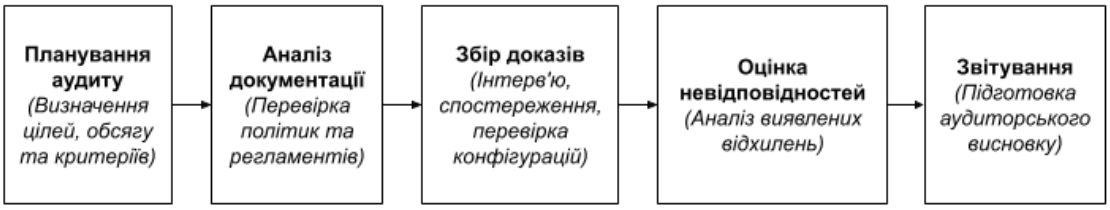

Рис. 1. Узагальнена схема процесу аудиту кібербезпеки

На етапі планування визначаються обсяг аудиту та критерії перевірки. Однак у динамічних середовищах реєстри активів часто втрачають актуальність ще до початку польового етапу. Процес збору доказів та оцінки відповідності при ручному виконанні ускладнюється необхідністю обробки великих масивів даних. Це може приводити до появи технічних помилок або хибних висновків про невідповідність, які вимагають тривалої ручної перевірки та суттєво уповільнюють загальний хід аудиту. Фінальний етап звітування часто страждає від розриву між зафіксованими технічними відхиленнями та реальною оцінкою бізнес-ризиків. Саме ці структурні обмеження традиційного процесу стають об'єктом оптимізації за допомогою інтелектуальних систем [3].

Сучасний науковий дискурс навколо аудиту кібербезпеки дедалі більше зміщується від теоретичних обговорень до експериментальної перевірки можливостей штучного інтелекту в реальних умовах. Аналіз публікацій за 2023 – 2025 роки свідчить про те, що інтеграція ШІ трансформує аудит з періодичної процедури "post-factum" у безперервний процес управління кіберстійкістю, де алгоритми не лише фіксують минулі помилки, а й прогнозують майбутні загрози [6 – 8].

Основою цієї трансформації стає перехід до динамічної оцінки ризиків. Традиційні методи аудиту часто спираються на статичні зрізи даних, які швидко втрачають актуальність в умовах сучасних кіберзагроз. Натомість новітні дослідження демонструють ефективність використання методів машинного навчання для динамічного розрахунку ризиків у реальному

часі [9]. Використання алгоритмів предиктивної аналітики дозволяє обробляти історичні дані про інциденти та поточні метрики системи, прогнозуючи ймовірність атак ще до їх початку. Емпіричні дані підтверджують, що такий підхід дозволяє організаціям переходити від реактивного усунення наслідків до проактивного управління вразливостями, знижуючи організаційні ризики значно ефективніше, ніж традиційні матриці ризиків, які заповнюються вручну раз на рік [6]. Цей підхід вже демонструє результати у промисловому секторі. Показовим прикладом ефективності автоматизації є кейс компанії Siemens Energy, яка впровадила платформу Industrial IoT для моніторингу глобальних виробничих активів. Використання хмарних сервісів для централізованого збору телеметрії дозволило скоротити час на ручний збір даних на 50 %, а також знизити витрати на обслуговування активів на 25 % завдяки предиктивному виявленню технічних аномалій та відхилень у процесах [10].

Логічним продовженням динамічної оцінки ризиків є впровадження систем безперервного моніторингу та реагування. Концепція безперервного аудиту (Continuous Auditing) стала можливою завдяки здатності нейромереж обробляти великі потоки даних у реальному часі, нівелюючи фактор людської втоми [11]. У дослідженні [7] було доведено, що системи на базі глибокого навчання здатні не лише фіксувати порушення політик, але й ініціювати процедури реагування. Показовим є досвід фінансового сектору. Згідно зі звітом JPMorgan Chase, стратегічне використання AI-платформ для аналізу даних та виявлення загроз дозволило банку згенерувати понад 1 мільярд доларів бізнес-цінності та суттєво скоротити час на обробку рутинних операцій, який раніше вимірювався тисячами годин людської праці [8]. Це підтверджує тезу про те, що ШІ є необхідним інструментом для подолання критичного часового розриву між початком атаки та її виявленням.

Висока ефективність моніторингу досягається завдяки використанню методів глибокого навчання для виявлення аномалій і загроз. У цій сфері дослідники фіксують беззаперечну перевагу методів навчання без учителя. Експерименти з використанням автоенкодерів для аудиту хмарних середовищ показали точність виявлення аномалій на рівні 98 % [12]. Цінність цього підходу полягає у відсутності потреби в розмічених даних про атаки, оскільки модель навчається розпізнавати "нормальну" поведінку системи і автоматично позначає будь-які відхилення як підозрілі, що дозволяє виявляти навіть атаки нульового дня. Подальший розвиток цих методів призвів до створення гібридних архітектур. Зокрема, інтеграція автоенкодерів з мережами довгої короткострокової пам'яті (LSTM) дозволяє не лише фіксувати поточні аномалії, але й здійснювати проактивне прогнозування збоїв у хмарних середовищах, забезпечуючи відмовостійкість системи на рівні, недосяжному для класичних алгоритмів [13]. Паралельно з цим, для аналізу коду смарт-контрактів та складних транзакцій високу ефективність демонструють графові нейронні мережі (GNN), які здатні моделювати потік даних у вигляді графа і виявляти вразливості, що залишаються непомітними для традиційних статичних аналізаторів [14].

Окрім суто технічного виявлення загроз, критично важливим аспектом залишається контроль відповідності та нормативний аналіз. Для задач, де необхідно чітко класифікувати стан системи як "відповідає" або "не відповідає" стандарту (наприклад, ISO/IEC 27001 або NIST SP 800-53), науковці рекомендують використовувати гібридні підходи. З одного боку, класичні алгоритми, такі як Random Forest, демонструють високу точність та інтерпретованість при класифікації активів критичної інфраструктури [15]. З іншого боку, для інтелектуальної обробки текстових даних доцільно використовувати великі мовні моделі (LLM), які, як показано в роботі [16], здатні ефективно верифікувати інформацію та виявляти невідповідності в неструктурованому контенті. В аналітичному дослідженні [17] доведено, що моделі сімейства GPT-4 здатні автоматизувати побудову графів знань з неструктурованих даних, демонструючи значно вищу семантичну точність порівняно з легковаговими моделями (такими як BERT або LLaMA 2). Такий підхід дозволяє автоматизувати найбільш рутинну частину аудиту – зіставлення технічних налаштувань та документів на вимоги регуляторів.

Логічним завершенням циклу повної автоматизації аудиту є оптимізація управлінських процесів та підтримка прийняття рішень. Дослідження показують, що автоматизація збору доказів та первинного аналізу може підвищити загальну ефективність аудиту. Більше того, ШІ починає відігравати роль інтелектуального асистента. Робота [18] описує системи підтримки рішень, які використовують машинне навчання для об'єктивної оцінки клієнтів та виявлення потенційного шахрайства ще на етапі планування аудиту. Яскравим прикладом є впровадження у банку Bradesco інтелектуального асистента AILA, що призвело до скорочення часу на планування аудиту на 65 % та прискорення підготовки звітів на 50 %, дозволяючи аудиторам фокусуватися на аналізі кореневих причин [19].

Найперспективнішим напрямком для повної автоматизації виконання технічних процедур без участі людини є використання агентних систем, де автономні агенти здатні самостійно виконувати перевірки в операційному середовищі. Дослідження [20] довело, що такі агенти можуть виконувати технічні аудиторські завдання швидше та точніше за людей, звільняючи експертів для прийняття стратегічних рішень. Зокрема, у сфері автоматизованого пошуку вразливостей застосування інструментів на базі ШІ дозволяє підвищити рівень виявлення загроз на 76 % та скоротити середній час усунення вразливостей (MTTR) на 65 %, хоча для виявлення складних логічних вразливостей та стратегічного мислення все ще необхідна участь людини [21]. Впровадження цих технологій, однак, вимагає вирішення проблеми надійності, зокрема схильності генеративних моделей до "галюцинацій" та забезпечення точності пріоритизації критичних ризиків, яка наразі сягає 89 % [21]. Окремим викликом стає забезпечення кіберстійкості самих агентів. Згідно з новітніми методологіями аудиту безпеки ШІ, автономні системи вимагають специфічного захисту від атак, спрямованих на маніпуляцію контекстом та несанкціоноване використання інструментів [22]. Емпіричні дані свідчать, що використання вдосконалених архітектур RAG (зокрема, інтеграція агентного ШІ та методу Multi-HyDE), які доповнюють генерацію пошуком по верифікованій базі знань, дозволяє підвищити точність відповідей на 11,2 % та знизити рівень галюцинацій на 15 %. Це відкриває шлях до безпечного використання ШІ не лише як інструменту аналізу, а й як засобу підвищення надійності роботи зі складною фінансовою документацією та регуляторними звітами. [23].

Для систематизації отриманих результатів було проведено порівняльний аналіз семи ключових технологічних напрямків ШІ, що застосовуються в аудиті (таблиця 1). Це дозволяє виділити специфічні ніші для кожного типу моделей та оцінити їхній вплив на аудиторські процедури.

Аналіз таблиці дозволяє простежити чітку еволюційну ієрархію методів. Традиційні підходи на основі правил залишаються фундаментом для комплаєнс-аудитів, де вимагається бінарна відповідь ("відповідає/не відповідає") та повна відтворюваність результатів. Водночас, зіставлення сильних та слабких сторін показує, що жоден метод ізольовано не покриває всі потреби аудиту. Саме це зумовлює необхідність переходу до гібридних архітектур, які компенсують «крихкість» жорстких правил адаптивністю машинного навчання.

Однак перехід до методів машинного навчання та обробки природної мови дозволяє змінити парадигму аудиту з простої фіксації порушень на проактивне прогнозування ризиків. Інструменти на базі ШІ забезпечують автоматизацію рутинних завдань, дозволяючи в реальному часі аналізувати великі масиви даних та виявляти приховані аномалії, які можуть залишитися непоміченими при традиційних методах перевірки. Це значно підвищує точність, ефективність та прогностичні можливості аудиту кібербезпеки [24]. Водночас, інтеграція інструментів на базі ШІ знаменує радикальну зміну в підходах до управління, уможливлюючи перехід до концепції Continuous Assurance (безперервної впевненості). Це дозволяє здійснювати аудит та оцінку ризиків у режимі реального часу, забезпечуючи превентивне виявлення загроз та значне підвищення операційної ефективності перевірок [7].

Таблиця 1

Порівняльна характеристика підходів ШІ до автоматизації аудиту кібербезпеки

Підхід	Типові завдання в аудиті	Переваги	Обмеження та ризики	Приклад застосування
Автоматизація на основі правил	Збір доказів, перевірка конфігурацій за чек-листами (CIS, NIST), моніторинг доступу.	Висока точність і передбачуваність; прозорість рішень; ідеально для рутинних задач.	Нездатність адаптуватися до нових загроз; "крихкість" при зміні IT-середовища; високий рівень хибних спрацювань.	Автоматизована перевірка налаштувань AWS на відповідність ISO 27001 (Vanta, Drata) [25]
Навчання з вчителем	Оцінювання ризиків, виявлення відомих типів шахрайства, класифікація транзакцій.	Ефективна обробка великих даних; зниження ручного навантаження; точність на знайомих патернах.	Потребує великих обсягів розмічених даних для навчання; ризик упередженості навчальних даних.	KPMG Clara для визначення рівня ризику транзакцій та оцінки фінансових ризиків [26]
Навчання без вчителя	Виявлення аномалій, пошук загроз "нульового дня".	Здатність виявляти невідомі загрози без попереднього навчання на атаках; робота з неструктурованими даними.	Проблема "чорної скриньки" (низька пояснюваність рішень); можлива висока кількість аномалій, що не є загрозами.	Darktrace Enterprise Immune System для виявлення аномальної поведінки [27]
Навчання з підкріпленням	Автономне тестування на проникнення, динамічне налаштування політик безпеки.	Навчання через взаємодію; виявлення складних ланцюжків атак; робота без розмічених датасетів	Висока складність навчання; ризик збоїв при навчанні на "живих" системах; ресурсоємність.	DeepExploit [28]
Генеративний ШІ/ ВММ	Генерація звітів, аналіз нормативної документації, інтерпретація логів.	Розуміння контексту; здатність пояснювати складні технічні проблеми простою мовою.	Ризик "галюцинацій" (фактичних помилок); ризики конфіденційності даних при використанні публічних моделей.	Deloitte Omnia для автоматичного створення чернеток аудиторських звітів [29]
Автономні ШІ агенти	Автономне тестування на проникнення, самостійне планування аудиту.	Повна автономність дій; здатність будувати ланцюжки атак; безперервний режим роботи (24/7).	Складність контролю дій агента; ризик непередбачуваних наслідків у виробничому середовищі.	Агенти для автоматизованого тестування на проникнення (PentestGPT) [30]

Окремим перспективним вектором розвитку є використання генеративного штучного інтелекту для вирішення проблеми дефіциту даних. Традиційні ML-моделі часто страждають від нестачі прикладів реальних атак для навчання. Новітні дослідження пропонують використовувати генеративного ШІІ для створення синтетичних даних, зокрема через фреймворки типу SAGA (Synthetic Audit log Generation for APT campaigns). Це дозволяє генерувати реалістичні логи складних атак, на яких навчаються захисні системи, що значно підвищує точність виявлення аномалій без ризику для реальної інфраструктури [31].

Крім того, відбувається еволюційний перехід від пасивних інструментів до агентних систем. Дослідження у сфері складних систем показують, що такі агенти здатні автономно виявляти та інтерпретувати аномалії без втручання людини, що трансформує роль аудитора з

оператора рутинних перевірок у наглядача за адаптивними, цілеспрямованими системами безпеки [32]. Важливим елементом тут виступають цифрові двійники, які дозволяють проводити агресивне стрес-тестування та аудит безпеки у віртуальній копії системи, не порушуючи безперервність бізнес-процесів основної інфраструктури [33].

Висновки

В результаті проведеного дослідження встановлено, що інтеграція штучного інтелекту в процеси аудиту кібербезпеки трансформує його з періодичної процедури контролю у безперервний процес управління кіберстійкістю. Аналіз показав, що найефективнішим сьогодні є застосування гібридних архітектур, які поєднують інтерпретованість експертних правил із адаптивністю алгоритмів глибокого навчання. Це дозволяє здійснити перехід до динамічної оцінки ризиків у реальному часі, нівелюючи критичний часовий розрив між виникненням атаки та її фіксацією, а також забезпечує виявлення аномалій "нульового дня" завдяки методам навчання без учителя.

Вагомим результатом роботи стало обґрунтування доцільності використання генеративного ШІ для вирішення проблеми дефіциту даних. Застосування синтетичних даних дозволяє моделювати сценарії складних атак для навчання захисних систем без ризику для реальної інфраструктури, а впровадження технології цифрових двійників відкриває можливості для безпечного стрес-тестування корпоративних мереж.

Водночас виявлено, що бар'єром для повної автоматизації залишається проблема надійності моделей, зокрема їх схильність до галюцинацій. Крім того, з переходом до використання автономних агентних систем виникає необхідність захисту самих інструментів аудиту. Критичним викликом стає забезпечення стійкості інтелектуальних агентів до зловмисних впливів та маніпуляцій контекстом, що вимагає впровадження спеціалізованих процедур тестування кібербезпеки ШІ.

У зв'язку з цим, перспективи подальших досліджень полягають у розробці стандартизованих фреймворків, які поєднують архітектури RAG, механізми Human-in-the-Loop та протоколи захисту агентів для безпечного розгортання систем автоматизованого аудиту.

СПИСОК ЛІТЕРАТУРИ

1. International Organization for Standardization. Guidelines for auditing management systems. 2018. URL: https://standards.iteh.ai/catalog/standards/iso/05ff9921-70ae-4e49-8423-29ab30e250cc/iso-19011-2018.

2. Grance T., Stevens M., Myers M. Guide to Selecting Information Technology Security Products. National Institute of Standards and Technology, 2003. URL: https://www.kennesaw.edu/coles/centers/cyber-center/resources/docs/nist-sp800-36.pdf.

3. Bharathan R. Automating IT audit evidence collection: Reducing risk and cost through ServiceNow integration. *International Journal of Science and Research Archive*. 2025. Vol. 16, №3. P. 1393–1401. URL: https://doi.org/10.30574/ijsra.2025.16.3.2584.

4. Mishra R. Enhancing IT audit readiness through automated evidence collection in Service Now. *Scientific Journal of Artificial Intelligence and Blockchain Technologies*. 2025. Vol. 2, №4. P. 1–6. URL: https://doi.org/10.63345/sjaibt.v2.i4.201.

5. Amodu O. Security auditors' perspective in tackling cyber-threats. *Journal of Multidisciplinary Engineering Science and Technology*. 2024. Vol. 11, №5. P. 16868–16872. URL: https://www.researchgate.net/publication/381280763.

6. Pycka M., Zastempowski M. Machine learning and artificial intelligence techniques adopted for IT audit. *Management*. 2025. Vol. 29, №1. P. 1–1. URL: https://doi.org/10.58691/man/200768.

7. Agboluaje R. AI-enhanced cybersecurity audits in IT governance: Strengthening risk management, compliance, and threat intelligence. *International Journal of Research Publication and Reviews*. 2025. Vol. 6, №2. P. 356–373. URL: https://doi.org/10.55248/gengpi.6.0225.0718.

8. Kitishian D. JPMorgan's AI Strategy: Chasing AI Dominance. URL: https://klover.ai/jpmorgan-ai-strategy-chasing-ai-dominance/.

9. Dynamic risk assessment approach for analysing cyber security events in medical IoT networks / R. M. Czekster et al. *Internet of Things*. 2025. Vol. 29. URL: https://doi.org/10.1016/j.iot.2024.101437.

10. Services A. W. Siemens Energy builds industrial IoT platform and drives smart manufacturing using AWS IoT.

URL: https://aws.amazon.com/solutions/case-studies/siemens-energy-video-case-study/.

11. Васюра А. С., Мартинюк Т. Б., Куперштейн Л. М. Методи та засоби нейроподібної обробки даних для систем керування. Вінниця : УНІВЕРСУМ-Вінниця, 2008. 175 с.

12. Peek inside the closed world: Evaluating autoencoder-based detection of DDoS to cloud / H. Guo et al. *arXiv*. 2020. URL: https://doi.org/10.48550/arXiv.1912.05590.

13. Pathania N., Singh B. Design of an integrated model using hybrid autoencoder and LSTM for fault tolerance and load balancing in cloud environments. *International Journal of Computer Networks and Applications*. 2024. Vol. 11, №6. P. 954–971. URL: https://doi.org/10.22247/ijcna/2024/57.

14. Smart contract vulnerability detection using graph neural network / Y. Zhuang et al. *Proceedings of the Twenty-Ninth International Joint Conference on Artificial Intelligence*. 2020. P. 3283–3290. URL: https://doi.org/10.24963/ijcai.2020/454.

15. Roy D., Sony R. I., Bhuiyan M. A. I. Advanced Strategies for Substation Asset Management: Leveraging Artificial Intelligence and Predictive Analytics. *Journal of Computer Science and Technology Studies*. 2025. Vol. 7, №11. P. 84–110. URL: https://doi.org/10.32996/jcsts.2025.7.11.12.

16. AI-agent-based system for fact-checking support using large language models / L. Kupershtein et al. *Proceedings of the 7th Workshop for Young Scientists in Computer Science & Software Engineering (CS&SE@SW 2024)*. 2024. P. 321–331. URL: https://ceur-ws.org/Vol-3917/paper50.pdf.

17. Bhatt A., Vaghela N., Dudhia K. Generating knowledge graphs from large language models: A comparative study of GPT-4, LLaMA 2, and BERT. *arXiv*. 2024. URL: https://doi.org/10.48550/arXiv.2412.07412.

18. Development of a decision support system for client acceptance in independent audit process / S. Cebi et al. *International Journal of Accounting Information Systems*. 2024. Vol. 53. URL: https://doi.org/10.1016/j.accinf.2024.100683.

19. Microsoft. Audit of the future: Bradesco increases efficiency by 65\% with Microsoft Azure. URL: https://customers.microsoft.com/en-us/story/24561-bradesco-bank-azure-openai.

20. Salodkar A. Transforming audit and regulatory compliance with AI agents. URL: https://doi.org/10.2139/ssrn.5512498.

21. Akinyemi A. M., Sims S. Role of artificial intelligence in modern cybersecurity vulnerability management practices. *World Journal of Advanced Research and Reviews*. 2025. Vol. 26, №1. P. 555–584. URL: https://doi.org/10.30574/wjarr.2025.26.1.1028.

22. Ajayi S. AI Security Auditing Methodology (Version 1.0). URL: https://docs.hacken.io/methodologies/AI_Red_Team/.

23. Enhancing financial RAG with agentic AI and multi-HyDE: A novel approach to knowledge retrieval and hallucination reduction / A. G. Srinivasan et al. *Indian Institute of Technology Madras*. 2025. URL: https://doi.org/10.48550/arXiv.2509.16369.

24. Zhang C., Cho S., Vasarhelyi M. Explainable Artificial Intelligence (XAI) in auditing. *International Journal of Accounting Information Systems*. 2022. Vol. 46. URL: https://doi.org/10.1016/j.accinf.2022.100572.

25. Towards automated continuous security compliance. ESEM '24: Proceedings of the ACM / F. Angermeir et al. *IEEE International Symposium on Empirical Software Engineering and Measurement*. 2024. URL: https://doi.org/10.1145/3674805.3690748.

26. KPMG Auditores S.L. Audit quality: Building trust. URL: https://assets.kpmg.com/content/dam/kpmgsites/es/pdf/2025/07/audit-quality-building-trust-2025.pdf.coredownload.inline.pdf.

27. Darktrace. Machine learning: A higher level of automation. URL: https://cstor.com/wp-content/uploads/2016/10/Darktrace_Machine-Learning_White-Paper.pdf.

28. Horizon3.ai. The shortcomings of traditional penetration tests – and how autonomous pentesting addresses them. URL: https://horizon3.ai/wp-content/uploads/2022/07/IDC_Report___The_Shortcomings_of_Traditional_Penetration_Tests.pdf.

29. Bramwell J. Deloitte expands GenAI, agentic AI capabilities for its auditors. CPA Practice Advisor. 2025. URL: https://www.cpapracticeadvisor.com/2025/07/16/deloitte-expands-genai-and-agentic-ai-capabilities-for-its-auditors/164990/.

30. Куперштейн Л. М., Притула А. В., Маліновський В. І. Аналіз технологій тестування на проникнення web-додатків. *Наукові праці Вінницького національного технічного університету*. 2024. № 2. URL: https://doi.org/10.31649/2307-5376-2024-2-45-53.

31. SAGA: Synthetic audit log generation for APT campaigns / Y.-T. Huang et al. *arXiv*. 2024. URL: https://doi.org/10.48550/arXiv.2411.13138.

32. Vatankhah Barenji R., Khoshgoftar S. Agentic AI for autonomous anomaly management in complex systems. *arXiv*. 2025. URL: https://doi.org/10.48550/arXiv.2507.15676.

33. Repetto M. Cybersecurity digital twins: Concept, blueprint, and challenges for multi-ownership digital service chains. *Journal of Information Security and Applications*. 2026. Vol. 96. Article 104299. URL: https://doi.org/10.1016/j.jisa.2025.104299.

Стаття надійшла до редакції 10.02.2026.
Стаття пройшла рецензування 17.03.2026.
Стаття опублікована 31.03.2026.

Куперштейн Леонід Михайлович – канд. техн. наук, доцент кафедри захисту інформації, ORCID: 0000-0001-6737-7134, e-mail: kupershtein@vntu.edu.ua.

Волинець Віталій Володимирович – аспірант кафедри захисту інформації, ORCID: 0009-0006-7999-1290, e-mail: volynets1026@gmail.com.
Вінницький національний технічний університет.

Войтович Олеся Петрівна – канд. техн. наук, доцент кафедри захисту інформації, ORCID: 0000-0001-8964-7000, e-mail: voytovych.olesya@vntu.edu.ua.
Вінницький національний аграрний університет.