АКТУАЛЬНІ ПИТАННЯ ЕКОНОМІЧНИХ НАУК

Менеджмент

УДК 005.8:004.42:004.7

DOI https://doi.org/10.5281/zenodo.19657428

Автоматизація процедур внутрішнього аудиту ризиків кібербезпеки за допомогою засобів машинного навчання та великих даних

Куницька Інна Володимирівна,
асистент кафедри економічної кібернетики, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м. Київ, Україна, https://orcid.org/0009-0009-7896-5754

Жидовська Наталія Михайлівна,
кандидат економічних наук, доцент кафедри обліку і оподаткування, Львівський національний університет ветеринарної медицини та біотехнологій імені С.З. Ґжицького, м. Львів, Україна, https://orcid.org/0000-0002-1883-5992

Фадєєва Ірина Георгіївна,
доктор економічних наук, професор, професор кафедри фінансів, обліку та оподаткування, Інститут економіки та менеджменту, Івано-Франківський національний технічний університет нафти і газу, м. Івано-Франківськ, Україна, https://orcid.org/0000-0002-6978-1621

Прийнято: 13.03.2026 | Опубліковано: 30.03.2026

Анотація. Українські підприємства активно інтегрують цифрові технології в бізнес-процеси, що супроводжується зростанням кількості кіберзагроз та підвищує вимоги до ефективності внутрішнього аудиту для

своєчасного виявлення аномалій та мінімізації потенційних втрат. **Метою статті** є розроблення моделі автоматизації процедур внутрішнього аудиту ризиків кібербезпеки на основі методів машинного навчання та технологій великих даних із визначенням критеріїв оцінювання їх ефективності. **Методи.** У роботі використано загальнонаукові методи аналізу, синтезу, індукції та дедукції для узагальнення теоретичних підходів до автоматизації внутрішнього аудиту ризиків кібербезпеки, моделювання – для розроблення структури автоматизованої системи, експерименту – для перевірки результативності запропонованої моделі на практичних даних. **Результати.** Охарактеризовано особливості автоматизації процедур внутрішнього аудиту ризиків кібербезпеки з використанням технологій машинного навчання та аналізу великих даних, що дає змогу підвищити точність і швидкість виявлення кіберінцидентів та оцінити загрози. Встановлено, що сучасні підходи до внутрішнього аудиту в українських і міжнародних практиках формуються на базі стандартів ISO (серія ISO/IEC 27001), NIST Cybersecurity Framework (CSF), COBIT 2019/ISACA, ITAF/ISACA, COSO (ERM 2017), що забезпечує структуровану основу для контролю кіберризиків і підтримки управлінських рішень. З'ясовано, що класифікаційні алгоритми Random Forest та SVM є ефективними для автоматизованого виявлення інцидентів безпеки, а методи кластеризації K-means і DBSCAN допомагають ідентифікувати аномалії в поведінці користувачів та мережевих потоках. Показано, що застосування методів глибинного навчання для аналізу багатовимірних кіберзагроз і технологій обробки природної мови для опрацювання текстових політик та аудиторських звітів передбачає комплексну ідентифікацію та оцінювання ризиків кібербезпеки. Доведено, що впровадження цифрового аудиторського двійника, адаптивного ризик-скорингу в реальному часі, self-learning аудит-контролів та ШІ-асистента внутрішнього аудитора окреслює інтеграцію алгоритмів аналізу даних у систему управління інформаційною безпекою підприємства та збільшує ефективність безперервного моніторингу

 ISSN 3041-2129

ризиків. **Висновок.** Визначено, що інтеграція методів машинного навчання та технологій великих даних у процедури внутрішнього аудиту ризиків кібербезпеки гарантує підвищення точності ідентифікації та прогнозування загроз, а також трансформацію аудиту з ретроспективного контролю у формат безперервного моніторингу й адаптивного управління ризиками.

Ключові слова: кіберзагрози, алгоритми, класифікація, аномалії, прогнозування, моделювання, інциденти, оптимізація, контекст, адаптивність.

Automating internal cybersecurity risk audit procedures using machine learning and big data

Inna Kunytska,
Assistant, Department of Economic Cybernetics, National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute», Kyiv, Ukraine, https://orcid.org/0009-0009-7896-5754

Nataliia Zhydovska,
PhD in Economics, Associate Professor of the Department of Accounting and Taxation, Stepan Gzhytskyi National University of Veterinary Medicine and Biotechnologies Lviv, Lviv, Ukraine, https://orcid.org/0000-0002-1883-5992

Iryna Fadyeyeva,
Doctor of Economics Habilitated, Professor, Department of Finance, Accounting and Taxes, Institute of Economics and Management, Ivano-Frankivsk National Technical University of Oil and Gas, Ivano-Frankivsk, Ukraine, https://orcid.org/0000-0002-6978-1621

Abstract. Ukrainian enterprises are actively integrating digital technologies into business processes, which is accompanied by an increase in cyber threats and

heightens the need for efficient internal audit to detect anomalies in a timely manner and minimize potential losses. The **purpose of the article** is to develop a model for automating internal audit procedures for cybersecurity risks using machine learning methods and big data technologies, and to define criteria for assessing their effectiveness. **Methods**. The work uses general scientific methods of analysis, synthesis, induction, and deduction to develop theoretical approaches to the automation of internal audit of cybersecurity risks, to model the structure of an automated system, and to experimentally verify the effectiveness of the proposed model on practical data. **Results**. The features of automating internal audit procedures for cybersecurity risks using machine learning and big data analysis technologies are characterized, enabling greater accuracy and faster cyber incident detection and threat assessment. It has been established that modern approaches to internal audit in Ukrainian and international practices are formed on the basis of ISO standards (ISO/IEC 27001 series), NIST Cybersecurity Framework (CSF), COBIT 2019/ISACA, ITAF/ISACA, COSO (ERM 2017), which provides a structured basis for controlling cyber risks and supporting management decisions. It has been found that the Random Forest and SVM classification algorithms are effective for automated detection of security incidents, and the K-means and DBSCAN clustering methods allow identifying anomalies in user behavior and network flows. It has been shown that the use of deep learning methods for analyzing multidimensional cyber threats and natural language processing technologies for processing text policies and audit reports provides comprehensive identification and assessment of cybersecurity risks. It was found that implementing a digital audit twin, adaptive real-time risk scoring, self-learning audit controls, and an AI assistant for the internal auditor ensures the integration of data analysis algorithms into the enterprise's information security management system and increases the effectiveness of continuous risk monitoring. **Conclusions**. It was found that integrating machine learning methods and big data technologies into internal audit procedures for cybersecurity risks increases the accuracy of threat identification and forecasting, and transforms the

audit from a retrospective control to a continuous monitoring and adaptive risk management model.

Keywords: cyber threats, algorithms, classification, anomalies, prediction, modeling, incidents, optimization, context, adaptability.

Постановка проблеми. У сучасних умовах розвитку інформаційних технологій бізнес-процеси українських підприємств стають дедалі більш цифровізованими, що водночас підвищує ризики для інформаційної безпеки. Внутрішній аудит кіберризиків у таких організаціях набуває критичного значення, оскільки від його ефективності залежить не лише збереження фінансових ресурсів, а й захист конфіденційної інформації та підтримка довіри клієнтів і партнерів. Поширення складних цільових атак, використання нових методів фішингу та витоку даних демонструє, що традиційні підходи до аудиту ризиків не завжди здатні адекватно реагувати на швидкі зміни в кіберпросторі, що потребує інтеграції автоматизованих технологій для поліпшення точності й оперативності оцінювання загроз.

Водночас застосування алгоритмів машинного навчання (МН) та аналітики великих даних (ВД) відкриває можливості для безперервного моніторингу інформаційних систем підприємств, забезпечуючи своєчасне виявлення аномалій і потенційних кіберзагроз. Розпізнавання поведінкових патернів користувачів, аналіз логів серверів і мережевих пристроїв, а також моделювання сценаріїв атак дає змогу сформувати більш глибоке та контекстуально обґрунтоване уявлення про ризики.

Отже, складність сучасних кіберзагроз і швидкість технологічних змін потребують створення адаптивних моделей внутрішнього аудиту, які можуть інтегрувати інтелектуальні алгоритми у вже наявні системи управління ризиками. Однак відсутність узгоджених підходів до валідації алгоритмів МН, недостатня якість даних для навчання моделей та мало методів оцінювання ефективності автоматизованих процедур створюють серйозні перепони для їх

практичного застосування. Усвідомлення цих викликів дає змогу окреслити пріоритети подальших досліджень, спрямованих на підвищення надійності й ефективності внутрішнього аудиту кіберризиків, а також формування методологічного підґрунтя для впровадження інноваційних інструментів у різних сферах діяльності підприємств.

Аналіз останніх досліджень і публікацій. Внутрішній аудит кіберризиків у сучасних умовах розглядають із позицій ризик-орієнтованого підходу, цифрової трансформації бізнес-процесів і використання інтелектуальних технологій аналізу даних. У дослідженні А. М. Десятко, В. Ф. Гамалія та Р. А. Ширшова запропоновано модель інтеграції корпоративних даних, IT-рішень та аудиторських процедур у межах єдиної архітектури управління, де якість аудиторських висновків прямо залежить від повноти даних і рівня автоматизації їх обробки [1]. Розроблена концепція передбачає централізоване агрегування інформації з різних підсистем підприємства та її аналітичне опрацювання в режимі, наближеному до реального часу.

У роботі В. Ободяка, М. Отрощенка та В. Любчака обґрунтовано застосування алгоритмів машинного навчання (навчання з учителем, без учителя та з підкріпленням) для аналізу великих масивів даних у сфері кібербезпеки, зокрема для виявлення аномалій мережевого трафіку, класифікації інцидентів і прогнозування ризикових подій [2]. Модульну систему оцінювання кіберризиків корпоративних мереж із використанням самоорганізованих алгоритмів демонструють І. Рамський (I. Ramskyi), А. Дрозд (A. Drozd), О. Лигун (O. Lyhun) та О. Поночовна (O. Ponochovna), що дає змогу адаптувати параметри моделей до змін у структурі мережі та поведінкових характеристиках користувачів [3].

Автоматизацію планування аудиту та визначення ризиків із застосуванням методів машинного навчання показано в праці С. В. Івахненкова (S. V. Ivakhnenkov) [4], де алгоритмічна підтримка

забезпечує формування ризик-орієнтованих програм перевірки. Роль аналітики великих даних і необхідність аудиту самих алгоритмів машинного навчання як об'єкта контролю підкреслено в роботі Н. Приймак [5]. Інтеграцію ERP-систем, хмарних платформ та технологій виявлення аномалій для підвищення прозорості й аналітичної глибини аудиторських процедур аргументувала К. Янковська [6].

Ефективність використання агентів штучного інтелекту для автоматизованого тестування програмних систем висвітлюють І. Письменний (I. Pysmennyi), Р. Кислий (R. Kyslyi) та К. Клещ (K. Kleshch), акцентуючи увагу на ризиках непрозорості моделей типу чорної скриньки [7]. Багаторівневу архітектуру інтелектуальної системи внутрішнього аудиту із застосуванням ансамблевих моделей прогнозування та API-інтеграції пропонують Д. Д. Гнатченко та А. М. Десятко [8]. Технічні аспекти розгортання моделей штучного інтелекту в корпоративному середовищі з використанням контейнеризації та мікросервісної архітектури для забезпечення відмовостійкості й обробки даних у режимі реального часу обґрунтовують Ю. Берщанський (Y. Bershchanskyi), Г. Клим (H. Klym) та Ю. Шевчук (Y. Shevchuk) [9]. Ефективність гібридної багаторівневої моделі тестування кіберзагроз доведено в дослідженні Д. Кияшка (D. Kyiashko) [10].

Узагальнення наведених підходів показує, що наукові пошуки зосереджені переважно на технологічних аспектах застосування машинного навчання, великих даних та інтелектуальних агентів у кібербезпеці. Водночас питання їх системної інтеграції безпосередньо в методологію внутрішнього аудиту з урахуванням організаційних процедур, регламентів контролю та управлінської інтерпретації результатів потребує подальшого наукового обґрунтування.

Виділення невирішених раніше частин загальної проблеми. Аналіз наукових джерел свідчить про те, що впровадження технологій МН та ВД суттєво змінює концепцію внутрішнього аудиту ризиків кібербезпеки,

переводячи його з періодичних перевірок у площину безперервного моніторингу й аналітично обґрунтованої підтримки управлінських рішень. Попри це, у науковому дискурсі зберігаються теоретико-методологічні прогалини, зокрема недостатньо розроблено концептуальні засади інтеграції алгоритмів МН в методологію внутрішнього аудиту, що не дає змоги сформувати узагальнену теоретичну модель їх застосування. Майже немає цілісних міждисциплінарних теоретичних моделей, які б системно поєднували аналіз впливу технічних, організаційних та поведінкових чинників управління ризиками кібербезпеки. Розроблення теоретичних підходів до оцінювання довгострокової ефективності автоматизованих систем аудиту, зокрема в контексті їх адаптивності до динамічних кіберзагроз, та концептуалізація категоріально-понятійного апарату автоматизації внутрішнього аудиту на основі МН та ВД також потребують доопрацювання.

Отже, актуалізується потреба у створенні адаптивних теоретичних моделей автоматизації внутрішнього аудиту ризиків кібербезпеки, здатних гарантувати методологічну цілісність і концептуальну узгодженість досліджень у цій сфері.

Формулювання цілей статті (постановка завдання). Мета статті – дослідити теоретичні та практичні аспекти автоматизації процедур внутрішнього аудиту ризиків кібербезпеки із застосуванням технологій МН та ВД, визначити їх вплив на ефективність системи управління інформаційною безпекою підприємства, а також обґрунтувати напрями вдосконалення аудиторських процесів в умовах цифрової трансформації.

Завдання статті:

1. Проаналізувати сучасні підходи до внутрішнього аудиту ризиків кібербезпеки, зокрема в контексті міжнародних стандартів та практик.

2. Вивчити можливості застосування технологій МН та ВД для автоматизованого виявлення, оцінювання та моніторингу кіберризиків у процесі внутрішнього аудиту.

3. Розробити практичні рекомендації щодо впровадження автоматизованих інструментів аудиту, ураховуючи інтеграцію алгоритмів аналізу даних у систему управління інформаційною безпекою підприємства, та оцінити їх економічну й організаційну ефективність.

Виклад основного матеріалу дослідження. У сучасному цифровому середовищі внутрішній аудит набуває стратегічного значення, оскільки стає не лише механізмом перевірки відповідності процедурам, а інструментом управління ризиками та підтримки ухвалення обґрунтованих управлінських рішень. Згідно з підходами Institute of Internal Auditors, внутрішній аудит інтерпретують як незалежну професійну діяльність, спрямовану на підвищення якості управлінських процесів, надійності контрольного середовища й розвитку практик ризик-менеджменту та корпоративного врядування [11, с. 109].

У цифровізованих організаціях внутрішній аудит усе більше орієнтується на випереджальне виявлення загроз, насамперед у галузі ІТ та кіберпросторі, оскільки саме вони визначають стійкість підприємства. Така переорієнтація дає змогу інтегрувати оцінювання контрольних механізмів з аналізом ризикових сценаріїв, формуючи підґрунтя для своєчасного зниження потенційних втрат [12, с. 51]. Особливу увагу приділено загрозам, пов’язаним із порушенням конфіденційності, цілісності та доступності інформації, оскільки саме ці параметри є основою інформаційної безпеки.

Узагальнення зазначених аспектів дає можливість бачити кіберризиковий профіль організації цілісно та окреслює методологічні передумови для цифровізації процедур внутрішнього аудиту із застосуванням сучасних аналітичних рішень, зокрема методів МН та обробки ВД. Аналіз міжнародних стандартів і кращих практик у сфері кібербезпеки допомагає охарактеризувати сильні й слабкі сторони різних методологій та обґрунтувати інтеграцію новітніх технологій для забезпечення системності, прозорості аудиторських процедур і підвищення точності оцінювання ризиків (табл. 1).

Таблиця 1

Міжнародні стандарти до внутрішнього аудиту кіберризиків

Стандарт / організація	Основна спрямованість	Підхід до оцінювання кіберризиків	Особливості ВА
ISO (серія ISO/IEC 27001)	Система управління інформаційною безпекою	Ризик-орієнтований підхід, ідентифікація активів, загроз і вразливостей	Регулярні ВА ISMS, документування невідповідностей
NIST Cybersecurity Framework (CSF)	Управління кіберризиками на основі функціональної моделі	Категоризація ризиків та визначення рівня зрілості процесів	Самооцінка та аудит зрілості контролів безпеки
COBIT 2019/ISACA	Корпоративне управління IT та контроль	Оцінювання IT-ризиків через систему контролів і показників ефективності	Аудит IT-процесів, використання метрик та KPI
ITAF/ISACA	Професійні стандарти IT-аудиту	Характеристика ризиків через аудиторські процедури та доказову базу	Чітка методологія проведення внутрішнього IT-аудиту
COSO (ERM 2017)	Інтегроване управління ризиками підприємства	Інтеграція кіберризиків у загальну систему ERM	Аудит у межах загальної системи внутрішнього контролю

Джерело: авторська розробка [13; 14;15; 16; 17]

Міжнародні стандарти пропонують різні методології внутрішнього аудиту кіберризиків, які організації обирають і адаптують залежно від технічних можливостей, розміру та сфери діяльності. Так, ISO (серія ISO/IEC 27001) [13] пропонує ризик-орієнтований підхід через ідентифікацію активів, вразливостей і загроз, що забезпечує універсальність та міжнародне визнання, водночас збільшуючи вимоги до документування [14]. NIST Cybersecurity Framework (CSF) [15] визначає п’ять етапів планування аудиту: ідентифікація, захист, виявлення, реагування та відновлення, що дає змогу окреслювати як технічні, так і процедурні аспекти безпеки за умови адаптації до локальних

нормативів. COBIT 2019 [16] орієнтує аудит на корпоративне управління IT через KPI та контрольні механізми, підвищуючи вимірюваність оцінки, але потребує високого рівня знань і ресурсів. ITAF встановлює професійні стандарти IT-аудиту, що гарантує точність оцінювання ризиків, проте має обмежену практичну користь для нефахівців. COSO (ERM 2017) [17] інтегрує кіберризики в загальну систему управління ризиками підприємства, забезпечуючи узгодженість із корпоративним контролем, хоча не дає глибокої спеціалізації саме у сфері кібербезпеки.

Отже, вибір стандарту визначається специфікою організації, наявними ресурсами, цілями та регуляторними вимогами, а поєднання різних підходів дає змогу формувати комплексну й адаптивну систему внутрішнього аудиту, що поєднує технічне характеризування ризиків з інтеграцією в корпоративні процеси управління.

Методики аудиту інформаційної безпеки – це системний процес оцінювання захищеності інформаційних активів, що поєднує нормативні вимоги, ризик-орієнтований підхід та аналітичні процедури. Вони охоплюють перевірку відповідності політикам безпеки, аналіз архітектури інформаційних систем, контроль доступу, управління інцидентами та визначення кіберстійкості організації. Сучасний аудит ґрунтується на принципі безперервності та передбачає використання автоматизованих інструментів моніторингу, аналізу журналів подій, тестування на проникнення й оцінювання вразливостей. Інтеграція технологій МН та ВД забезпечує оперативний збір і обробку інформації, ранжування ризиків за рівнем впливу та ймовірністю, збільшує точність висновків і зменшує вплив людського фактора. Завдяки цьому внутрішній аудит трансформується в проактивний механізм управління кіберризиками, що формує аналітичну основу для своєчасного ухвалення управлінських рішень і підвищення рівня інформаційної безпеки організації (табл. 2).

Таблиця 2

Можливості застосування технологій машинного навчання та великих даних у внутрішньому аудиті кіберризиків

Технологія / метод				
Сфера застосування	Типи даних	Практичний результат	Переваги	Обмеження
Класифікаційні алгоритми (Random Forest, SVM, Logistic Regression)				
Автоматизоване виявлення інцидентів безпеки	Журнали подій (logs), мережевий трафік, дані доступу	Ідентифікація підозрілої активності	Висока точність прогнозування	Потребує якісних навчальних вибірок
Методи кластеризації (K-means, DBSCAN)				
Виявлення аномалій у поведінці користувачів	Поведінкові патерни, історія входів	Визначення нетипових дій	Виявлення невідомих загроз	Чутливість до параметрів моделі
Глибинне навчання (Neural Networks, LSTM)				
Аналіз складних багатовимірних кіберзагроз	Великі масиви різнорідних даних	Прогнозування потенційних атак	Обробка ВД у режимі реального часу	Високі обчислювальні ресурси
Обробка природної мови (NLP)				
Аналіз текстових звітів аудиту, політик безпеки, повідомлень про інциденти	Текстові документи, e-mail, службові повідомлення	Виявлення ризикових формулювань та невідповідностей	Автоматизація аналізу документації	Потребує мовної адаптації
Технології ВД (Hadoop, Spark)				
Інтеграція та обробка великих потоків аудиторських даних	Big Data (SIEM-логи, IoT, хмарні сервіси)	Комплексний моніторинг ризиків	Масштабованість і швидкість обробки	Складність упровадження
Predictive analytics				
Оцінювання ймовірності виникнення кіберінцидентів	Історичні дані про атаки та вразливості	Формування карти ризиків	Підтримка ухвалення управлінських рішень	Залежність від повноти історичних даних

Джерело: авторська розробка [18, с. 4; 19, с. 8; 20, с. 2; 21, с. 6; 22, с. 2]

Розглядаючи застосування технологій МН та ВД у внутрішньому аудиті кіберризиків, важливо враховувати, що їх ефективність залежить від конкретної організаційної структури та доступності даних. Класифікаційні

алгоритми, такі як Random Forest, SVM та логістична регресія, використовують аналітичні підрозділи безпеки для автоматизованого виявлення інцидентів у журналах подій, мережевому трафіку та даних доступу, що дає змогу відстежувати підозрілу активність і своєчасно реагувати на потенційні загрози [18, с. 4]. Точність цих алгоритмів визначається якістю навчальних вибірок, тому для оптимальної роботи необхідно мати доступ до репрезентативних і достовірних даних із внутрішніх систем організації.

Методи кластеризації, такі як K-means і DBSCAN, застосовують для виявлення аномалій у поведінкових патернах користувачів, що допомагає відокремлювати нетипові дії від звичайної активності та ідентифікувати потенційні загрози [19, с. 8]. У цьому випадку точність результатів залежить від налаштувань параметрів моделей і характеру даних, що потребує ретельного контролю під час налаштування системи.

Глибинне навчання, включно з нейронними мережами та LSTM-моделями, забезпечує аналіз складних багатовимірних кіберзагроз, обробляючи великі масиви структурованих і неструктурованих даних, що надходять із серверів, мережевих пристроїв і систем моніторингу [20, с. 2]. Такі технології дають змогу прогнозувати потенційні атаки в режимі реального часу, але для їхнього впровадження необхідні значні обчислювальні ресурси й відповідна IT-інфраструктура.

Обробку природної мови використовують для аналізу текстових звітів, політик безпеки та повідомлень про інциденти, що допомагає виявляти ризикові формулювання, невідповідності в документації та потенційні джерела загроз. Ефективність цього підходу залежить від адаптації моделей до мови та специфіки корпоративних документів, що гарантує точність і своєчасність аналітичних висновків [21, с. 6].

Технології ВД, зокрема Hadoop і Spark, застосовують для інтеграції та обробки потоків аудиторських даних із різних джерел, ураховуючи SIEM-системи та IoT-пристрої, що забезпечує комплексний моніторинг ризиків. Їхнє

 ISSN 3041-2129

впровадження потребує значної інфраструктури та ресурсів, проте їхня інтеграція створює умови для системного та швидкого аналізу великих обсягів даних [22, с. 2].

Аналітика прогнозування дає змогу оцінювати ймовірність виникнення кіберінцидентів на основі історичних даних про атаки та вразливості, формуючи карти ризиків, які допомагають керівництву ухвалювати обґрунтовані управлінські рішення. Точність цих прогнозів залежить від повноти й достовірності накопичених даних, що необхідно брати до уваги при плануванні застосування цих технологій.

Отже, інтеграція методів МН та обробки ВД у внутрішній аудит кіберризиків формує передумови для підвищення точності оцінювання загроз, оперативного виявлення аномалій та більш обґрунтованого управління ризиками. Водночас отримані дані свідчать про зменшення впливу людського фактора та раціоналізацію використання ресурсів аудиторських підрозділів. Попри наявні технічні обмеження й потребу у відповідному кадровому та обчислювальному забезпеченні, застосування зазначених інструментів сприяє кращій результативності аудиту та посилює здатність організації адаптуватися до динамічних кіберзагроз.

З огляду на виявлене, для удосконалення внутрішнього аудиту кіберризиків рекомендовано поетапне впровадження й інших автоматизованих аналітичних інструментів, інтегрованих із наявною інфраструктурою управління інформаційною безпекою, що поліпшить системний аналіз загроз, оптимізацію процедур контролю та підвищить якість управлінських рішень.

Так, одним із найбільш ефективних інноваційних інструментів аудиту є створення цифрового двійника аудиторської системи як засобу моделювання ризикових сценаріїв на віртуальній копії IT-інфраструктури організації. Це допомагає тестувати потенційні інциденти, оцінювати їх імовірний вплив і коригувати контрольні механізми без втручання в реальне виробниче

 ISSN 3041-2129

середовище. Інтеграція такого інструменту із системами класу SIEM та платформами управління інформаційною безпекою через API гарантує узгодженість потоків даних і збільшує аналітичні можливості аудиторської функції.

Іншим підходом є впровадження адаптивного ризик-скорингу в режимі реального часу, що передбачає динамічне визначення рівня загроз на підставі потокових даних із серверів, мережевих пристроїв і журналів доступу. Застосування МН-алгоритмів у цьому процесі скорочує час реагування на інциденти та створює передумови для переходу до моделі безперервного аудиту.

Крім того, доцільним є використання self-learning контрольних механізмів, здатних автоматично оновлювати параметри оцінювання ризику на основі нових інцидентів і накопичених знань корпоративної бази даних. Така самоадаптація контрольного середовища сприяє зниженню повторюваності загроз і поступовому підвищенню рівня зрілості системи інформаційної безпеки.

Упровадження Predictive Compliance Engine дає змогу прогнозувати потенційні порушення політик безпеки до їх фактичного виникнення, інтегруючи ці прогнози з внутрішніми контрольними процедурами й політиками інформаційної безпеки, що мінімізує фінансові та репутаційні ризики. Додатково, ШІ-асистент для внутрішніх аудиторів автоматизує формування висновків і рекомендацій на основі даних із внутрішніх реєстрів та журналів подій, зменшуючи трудомісткість аудиторської роботи та допомагаючи фахівцям зосередитися на стратегічних завданнях організації.

Інтеграція ризик-орієнтованої карти вразливостей із аналітичними панелями дає змогу візуалізувати пріоритетні ризики, оптимізувати розподіл бюджету на інформаційну безпеку та підвищити прозорість управлінських рішень. Завдяки поєднанню цих інноваційних рішень внутрішній аудит кіберризиків стає більш точним, проактивним і стратегічно-орієнтованим, що

поліпшує ефективність управління інформаційною безпекою та гарантує організації здатність швидко адаптуватися до нових кіберзагроз.

Висновки. Встановлено, що поєднання міжнародних стандартів управління інформаційною безпекою та корпоративного IT-контролю ISO (серія ISO/IEC 27001), NIST Cybersecurity Framework (CSF), COBIT 2019/ISACA, ITAF/ISACA, COSO (ERM 2017) забезпечує уніфікацію критеріїв оцінювання кіберризиків і підвищує узгодженість процедур внутрішнього аудиту, формуючи цілісну методологічну основу його організації. Підтверджено, що застосування алгоритмів МН та аналітики ВД у внутрішньому аудиті поліпшує точність і швидкість виявлення інцидентів інформаційної безпеки завдяки використанню класифікаційних моделей, методів кластеризації та інструментів глибинного аналізу текстових і багатовимірних даних. Обґрунтовано доцільність переходу до моделі безперервного аудиту кіберризиків, що реалізується через інтеграцію потокового аналізу даних, адаптивного ризик-скорингу та автоматизованої ідентифікації аномалій у систему управління інформаційною безпекою. Водночас упровадження цифрового двійника аудиторської системи та ШІ-асистента внутрішнього аудитора сприяє підвищенню оперативності аналізу інцидентів, оптимізації контрольних процедур і прозорості ухвалення управлінських рішень у сфері кібербезпеки.

Перспективи подальших досліджень пов’язані з формалізацією методів кількісного оцінювання ефективності автоматизованих систем внутрішнього аудиту, а також із розширеним емпіричним тестуванням запропонованої моделі в різних галузях економіки з урахуванням вимог до пояснюваності алгоритмів штучного інтелекту.

Список використаних джерел

1. Десятко А. М., Гамалій В. Ф., Ширшов Р. А. Інформаційні технології та системи для організації внутрішнього аудиту підприємства. *Електронне*

фахове наукове видання «Кібербезпека: освіта, наука, техніка». 2025. Т. 1, № 29. С. 867–876. DOI: https://doi.org/10.28925/2663-4023.2025.29.947.

2. Ободяк В., Отрощенко М., Любчак В. Можливості штучного інтелекту для аудиту та управління ризиками кібербезпеки. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка».* 2025. Т. 1, № 29. С. 319–330. DOI: https://doi.org/10.28925/2663-4023.2025.29.872.

3. Ramskyi I., Drozd A., Lyhun O., Ponochovna O. System for cybersecurity evaluation of corporate networks. *Computer systems and information technologies.* 2025. № 2. P. 123–131. DOI: https://doi.org/10.31891/csit-2025-2-14.

4. Ivakhnenkov S. V. Application of artificial intelligence in auditing. *Naukma Scientific Papers. Economic Sciences.* 2023. Vol. 8, № 1. P. 54–60. DOI: https://doi.org/10.18523/2519-4739.2023.8.1.54-60.

5. Приймак Н. Адаптація обліку та аудиту до викликів цифрової економіки: вплив штучного інтелекту. *Acta Academiae Beregsasiensis. Economics.* 2025. № 10. С. 500–515. DOI: https://doi.org/10.58423/2786-6742/2025-10-500-515.

6. Янковська К. Цифрова трансформація обліку та аудиту на основі сучасних інформаційних систем. *Вісник Львівського національного екологічного університету. Серія «Економіка АІК».* 2025. № 32. С. 50–54. DOI: https://doi.org/10.31734/economics2025.32.050.

7. Pysmennyi I., Kyslyi R., Kleshch K. AI-driven tools in modern software quality assurance: an assessment of benefits, challenges, and future directions. *Technology audit and production reserves.* 2025. Vol. 3, № 2 (83). P. 44–54. DOI: https://doi.org/10.15587/2706-5448.2025.330595.

8. Гнатченко Д. Д., Десятко А. М. Реалізація обчислювального ядра інтелектуальної системи підтримки внутрішнього аудиту. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка».* 2025. Т. 4, № 28. С. 781–793. DOI: https://doi.org/10.28925/2663-4023.2025.28.781793.

9. Bershchanskyi Y., Klym H., Shevchuk Y. Containerized artificial intelligent system design in cloud and cyber-physical systems. *Advances in Cyber-Physical Systems.* 2024. Vol. 9, № 2. P. 151–157. DOI: https://doi.org/10.23939/acps2024.02.151.

10. Kyiashko D. Development of a hybrid testing framework for multimodal systems based on AI agents. *Наука і техніка сьогодні.* 2025. № 11 (52). С. 1774–1788. DOI: https://doi.org/10.52058/2786-6025-2025-11(52)-1774-1788.

11. Crucean A. C., Hategan C. D. Effects of the Covid-19 pandemic estimated in the financial statements and the auditor's report. *Audit Financiar.* 2021. Vol. 19, № 161. P. 105–118. DOI: https://doi.org/10.20869/auditf/2021/161/001.

12. Marashdeh Z., Alomari M. W., Khataybeh M., Alkhataybeh A. Female representation on the boards of directors of non-financial companies. *Journal of Governance and Regulation.* 2021. Vol. 10, № 2. P. 44–54. DOI: https://doi.org/10.22495/jgrv10i2art4.

13. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements. 2022. URL: https://www.iso.org/standard/27001 (дата звернення: 15.01.2026).

14. NIST Cybersecurity Framework (CSF) 2.0 – Cybersecurity Framework 2.0 – National Institute of Standards and Technology, U.S. Department of Commerce. URL: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf (дата звернення: 15.01.2026).

15. COBIT 2019. Framework: Governance and Management Objectives ISACA (Information Systems Audit and Control Association). URL: https://www.isaca.org/resources/cobit (дата звернення: 15.01.2026).

16. IT Audit Framework (ITAF), 5th Edition. *ISACA*. URL: https://store.isaca.org/s/store#/store/browse/detail/a2SVQ0000029jHh2AI (дата звернення: 15.01.2026).

17. Enterprise Risk Management. *Committee of Sponsoring Organizations of the Treadway Commission (COSO)*. 2017. URL: https://www.coso.org/guidance-erm (дата звернення: 15.01.2026).

18. Natesha B. V., Guddeti R. M. R. Adopting elitism-based genetic algorithm for minimizing multi-objective problems of IoT service placement in fog computing environment. *Journal of Network and Computer Applications.* 2021. Vol. 178. 102972. DOI: https://doi.org/10.1016/j.jnca.2020.102972.

19. Yuan S., Wu X. Deep learning for insider threat detection: Review, challenges and opportunities. *Computers Security.* 2021. Vol. 104. 102221. DOI: https://doi.org/10.1016/j.cose.2021.102221.

20. Dessì D., Recupero D. R., Sack H. An assessment of deep learning models and word embeddings for toxicity detection within online textual comments. *Electronics.* 2021. Vol. 10, № 7. 779. DOI: https://doi.org/10.3390/electronics10070779.

21. Medjek F., Tandjaoui D., Djedjig N., Romdhani I. Multicast DIS attack mitigation in RPL-based IoT-LLNs. *Journal of Information Security and Applications.* 2021. Vol. 61. 102939. DOI: https://doi.org/10.1016/j.jisa.2021.102939.

22. Ahmad R., Alsmadi I., Alhamdani W., Tawalbeh L. A comprehensive deep learning benchmark for IoT IDS. *Computers security.* 2022. Vol. 114. 102588. DOI: https://doi.org/10.1016/j.cose.2021.102588.