

УДК 004.056:004.8

Левченко В.О., здобувач
Миша М.А., здобувач
Петляк Н.С., д. філ., доцент
Хмельницький національний університет

ІНТЕГРАЦІЯ ШТУЧНОГО ІНТЕЛЕКТУ В ПРОЦЕС АУДИТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

У сучасних умовах зростання кіберзагроз традиційні підходи до аудиту інформаційної безпеки (ІБ) часто виявляються недостатньо ефективними. Складність ІТ-інфраструктур і великий обсяг даних ускладнюють виявлення прихованих аномалій та потенційних вразливостей. У зв'язку з цим актуальним стає застосування технологій штучного інтелекту (ШІ) для підвищення ефективності аудиту. Інструменти ШІ дозволяють автоматизувати обробку великих масивів даних, аналізувати журнали подій, оцінювати конфігурації систем безпеки та виявляти атипову активність користувачів [1].

Метою роботи є дослідження можливостей застосування ШІ на різних етапах аудиту ІБ та визначення переваг і ризиків такої інтеграції.

Аудит ІБ відповідає циклу PDCA (Plan–Do–Check–Act), що забезпечує постійне вдосконалення системи управління ІБ [2]. Інтеграція ШІ має враховувати основні принципи аудиту: об'єктивність, професіоналізм, конфіденційність і незалежність. За належного налаштування інтелектуальні системи здатні підвищити об'єктивність аналізу та зменшити вплив людського фактора.

Етап планування. На етапі планування визначаються цілі аудиту, оцінюються ризики та формується програма перевірки. Технології ШІ можуть застосовуватися для аналізу внутрішніх політик і нормативної документації, обробки великих обсягів даних та автоматизованого виявлення потенційних ризиків. Зокрема, методи обробки природної мови забезпечують швидке опрацювання текстових документів і підтримують комплексний аналіз даних із різних джерел. Ефективність таких систем значною мірою залежить від якості вхідної інформації.

Етап виконання аудиту. У процесі проведення аудиту перевіряється відповідність інформаційних систем вимогам безпеки та ефективність захисних механізмів. Інструменти ШІ можуть аналізувати журнали подій, мережевий трафік, поведінку користувачів і конфігурації систем, а також інтегрувати дані з SIEM, сканерів вразливостей і засобів тестування на проникнення. А використання алгоритмів машинного навчання дозволяє автоматично виявляти аномалії, підозрілу активність і потенційні канали витоку інформації.

Формування аудиторського звіту. ШІ може підтримувати структурування результатів аудиту, формування попередніх висновків і рекомендацій щодо усунення виявлених ризиків. За умов глибокої інтеграції такі системи здатні генерувати структурований звіт у напівавтоматичному режимі, однак остаточне підтвердження результатів повинно здійснюватися аудиторською групою.

Етап перевірки та вдосконалення. На завершальному етапі оцінюється ефективність проведеного аудиту та визначаються напрями вдосконалення процедур. Інтелектуальні системи можуть аналізувати досягнення цілей аудиту, узагальнювати зворотний зв'язок і формувати пропозиції щодо оптимізації програми аудиту. За умов постійного моніторингу такі технології сприяють переходу від періодичних перевірок до проактивного управління ІБ.

Для узагальнення можливостей використання ШІ на різних етапах аудиту доцільно систематизувати основні завдання та функції, що можуть бути автоматизовані. Узагальнену характеристику відповідних можливостей подано в таблиці 1.

Таблиця 1 - Основні можливості застосування ШІ в аудиті

Етап аудиту	Завдання	Можливості ШІ
планування	аналіз документації	автоматичний аналіз політик
	оцінка ризиків	аналіз великих масивів даних
виконання	аналіз журналів	виявлення аномалій
	перевірка конфігурацій	автоматична перевірка
перевірка	аналіз результатів	кластеризація інцидентів
удосконалення	формування рекомендацій	генерація звітів

Результати дослідження свідчать, що застосування ШІ в аудиті ІБ може суттєво підвищити ефективність аудиторських процесів. Інтелектуальні системи дозволяють автоматизувати рутинні операції, швидко обробляти великі обсяги даних і виявляти потенційні загрози. Що сприяє підвищенню точності аналізу, зменшенню впливу людського фактора та покращенню якості аудиторських висновків.

Список використаних джерел

1. Fajrillah F., et al. Improving Information System Audit Security through Artificial Intelligence (AI) Technology Integration. *Journal of Technology and Computer*. 2025. № 2 (2). pp. 88–92. URL: <https://journal.technolabs.co.id/index.php/jotechcom/article/view/54>.

2. Чалий О., Толюпа С. Порівняння міжнародних стандартів аудиту інформаційної безпеки з перспективою автоматизації. *Кібербезпека: освіта, наука, техніка*. 2025. № 3 (31). С. 579–588. DOI: 10.28925/2663-4023.2025.31.1046.