УДК 004.81

О. П. Войтович
І. Ю. Пилявець
Є. В. Радченко

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В АУДИТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Вінницький національний технічний університет

Анотація

Розглянуто можливості використання штучного інтелекту (ШІ) в аудиті, зокрема в аудиті інформаційної безпеки. ШІ стає важливим інструментом для підвищення ефективності аудиторських процесів, автоматизації рутинних завдань та зменшення людських помилок. У сфері інформаційної безпеки ШІ дозволяє оперативно виявляти кіберзагрози, аналізувати великі масиви даних у реальному часі, а також забезпечувати відповідність політикам і стандартам безпеки. Розглядаються основні технології, що дозволяють ШІ здійснювати моніторинг, виявлення аномалій та прогнозування ризиків. Водночас обговорюються потенційні виклики, пов'язані з етикою, прозорістю та конфіденційністю даних. Перспективи використання ШІ в аудиті інформаційної безпеки вказують на те, що він може значно покращити точність та швидкість аудиторських перевірок, проте потребує уваги до питань управління та відповідності вимогам. Інтеграція ШІ в цю галузь має потенціал стати ключовим елементом для забезпечення безпеки в сучасному цифровому світі.

Ключові слова: штучний інтелект, аудит, інформаційна безпека, автоматизація, кібербезпека, аудит відповідності, машинне навчання, моніторинг, аналіз даних, виявлення загроз.

Abstract

The possibilities of using Artificial Intelligence (AI) in auditing, particularly in information security audits, are discussed. AI is becoming an important tool for enhancing the effectiveness of audit processes, automating routine tasks, and reducing human errors. In the field of information security, AI allows for the timely detection of cyber threats, real-time analysis of large datasets, and ensuring compliance with security policies and standards. The key technologies that enable AI to perform monitoring, anomaly detection, and risk forecasting are considered. At the same time, potential challenges related to ethics, transparency, and data confidentiality are discussed. The prospects of using AI in information security auditing suggest that it can significantly improve the accuracy and speed of audit checks; however, attention is needed to management and compliance issues. The integration of AI into this field has the potential to become a key element in ensuring security in the modern digital world.

Keywords: artificial intelligence, audit, information security, automation, cybersecurity, compliance audit, machine learning, monitoring, data analysis, threat detection.

Вступ

З розвитком цифрових технологій і зростанням кількості кіберзагроз організації стикаються з необхідністю підвищення рівня інформаційної безпеки. Аудит інформаційної безпеки є важливим інструментом для забезпечення відповідності стандартам і політикам безпеки, проте традиційні методи аудиту є трудомісткими та часто неефективними для аналізу великих обсягів даних. Штучний інтелект дозволяє автоматизувати значну частину процесів, що відкриває нові можливості для аудиту ІБ. ШІ може аналізувати велику кількість даних швидше, виявляти приховані загрози і прогнозувати потенційні ризики. Метою даної роботи є розгляд основних аспектів і перспектив використання ШІ в аудиті, особливо в контексті інформаційної безпеки.

Результати дослідження

Штучний інтелект (ШІ) трансформує аудит, автоматизуючи завдання, які раніше вимагали значних зусиль і часу. ШІ здатен автоматично аналізувати звіти, перевіряти відповідність стандартам, а також виконувати рутинні операції, такі як перегляд транзакцій або обробка великих масивів даних [1]. Здатність ШІ обробляти та аналізувати величезні обсяги даних з високою

швидкістю дозволяє значно скоротити час проведення аудиторських перевірок. Це знижує кількість людських помилок, які часто виникають через монотонність ручної роботи [2].

Інший важливий аспект автоматизації – можливість для аудиторів зосередитися на стратегічних та складних завданнях, таких як оцінка ризиків та управління контролями. ШІ бере на себе повторювані завдання, забезпечуючи комплексний аналіз даних та попереджаючи потенційні помилки [3]. Згідно з даними Deloitte [4], ШІ може покращити контроль відповідності стандартам шляхом автоматичної перевірки даних на відповідність вимогам нормативних документів та внутрішніх політик компанії.

Один із ключових напрямків застосування ШІ в аудиті — це виявлення аномалій. Наприклад, ШІ може аналізувати транзакції, розпізнаючи нетипові патерни, які можуть свідчити про потенційні порушення. За допомогою таких інструментів, як обробка природної мови (NLP), ШІ також аналізує текстові документи або електронну пошту, шукаючи ключові ознаки ризику.

Важливо зазначити, що виявлення шахрайства та аномалій є особливо критичним в сфері інформаційної безпеки. Кіберзагрози, такі як фішингові атаки можуть залишитися непоміченими в традиційних системах моніторингу. ШІ забезпечує глибоке та детальне виявлення загроз, що допомагає уникнути можливих втрат [5]. Один із найбільш перспективних аспектів використання ШІ в аудиті — це можливість оцінки ризиків. За допомогою алгоритмів машинного навчання та штучних нейронних мереж ШІ здатен прогнозувати ризики, аналізуючи історичні дані та виявляючи тенденції, що вказують на майбутні загрози [6].

IBM демонструє приклади використання ШІ для виявлення загроз у режимі реального часу[7]. Ці системи аналізують поведінкові дані з мережі, виявляючи підозрілу активність ще до того, як вона перетвориться на загрозу [6]. Це дозволяє знизити втрати від потенційних атак та забезпечити безперервність роботи підприємств.

У сфері інформаційної безпеки важливою складовою є перевірка на відповідність стандартам, таким як ISO/IEC 27001. ШІ може полегшити цей процес, автоматизуючи перевірку дотримання політик і контролів безпеки. Системи штучного інтелекту можуть автоматично перевіряти налаштування конфігурацій та мережеві параметри на відповідність стандартам [7]. Це особливо корисно для великих організацій з розгалуженою IT-інфраструктурою, де перевірка всіх аспектів вручну є трудомістким завданням.

У майбутньому, з огляду на постійний розвиток кіберзагроз та появу нових стандартів, системи ШІ будуть грати ще важливішу роль у підтримці безпеки та відповідності вимогам. Моніторинг є однією з ключових функцій у сфері інформаційної безпеки. ШІ дозволяє організаціям здійснювати безперервний моніторинг подій, пов’язаних із безпекою, що є особливо важливим для великих мережевих інфраструктур, де будь-яке порушення може мати катастрофічні наслідки.

ШІ здатен аналізувати лог-файли, мережевий трафік, виявляти аномальні дії та попереджати аудиторів про можливі загрози ще до того, як вони завдадуть шкоди. Використовуючи технології, такі як глибинне навчання, ШІ може "навчитися" на основі попередніх інцидентів і покращити виявлення нових загроз. Також штучний інтелект може використовуватися для прогнозування майбутніх загроз на основі минулих даних. Машинне навчання допомагає системам вивчати попередні атаки та використовувати цю інформацію для виявлення потенційних вразливостей у майбутньому, що дозволяє завчасно реагувати на ризики.

З часом штучний інтелект продовжуватиме розвиватися, що дозволить повністю автоматизувати процеси аудиту інформаційної безпеки. Це зменшить час на проведення перевірок, підвищить їх точність та забезпечить цілодобовий моніторинг. Gartner вказує на те, що використання ШІ в аудиті може значно розширити можливості щодо виявлення ризиків і відповідності вимогам. Оскільки все більше організацій використовують хмарні сервіси, важливим завданням є забезпечення їхньої безпеки. ШІ дозволяє автоматично перевіряти налаштування хмарних сервісів та забезпечувати їх відповідність політикам безпеки, що забезпечує надійний захист даних у нових технологічних середовищах .

Висновки

Штучний інтелект має величезний потенціал для розвитку аудиторських процесів, особливо у сфері інформаційної безпеки. Використання ШІ дозволяє підвищити ефективність, точність і швидкість аудиторських перевірок, забезпечити моніторинг і виявлення загроз у реальному часі, а також прогнозувати майбутні ризики. Однак, інтеграція ШІ в аудит вимагає врахування етичних питань та ризиків, пов’язаних із конфіденційністю даних. У майбутньому штучний інтелект стане невід'ємною частиною аудиту інформаційної безпеки, що значно підвищить рівень захисту в цифровому середовищі.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Artificial Intelligence projects from Deloitte Practical cases of applied AI. URL: https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/innovatie/deloitte-nl-innovatie-artificial-intelligence-16-practical-cases.pdf

2. Balancing Power and Protection: AI in Cybersecurity and Cybersecurity in AI - PwC Middle East. PwC. URL: https://www.pwc.com/m1/en/publications/balancing-power-protection-ai-cybersecurity.html.

3. European Commission. Auditing Artificial Intelligence: A Guide for Practitioners and Policymakers. 2020. URL: https://ec.europa.eu/futurium/en/system/files/ged/auditing-artificial-intelligence.pdf

4. Ethical considerations in the use of AI for auditing: balancing innovation and integrity. European journal of accounting, auditing and finance research. 2022. Vol. 10, no. 12. P. 91–108. URL: https://eajournals.org/ejaafr/wp-content/uploads/sites/16/2024/06/Ethical-Considerations.pdf.

5. Badman A., Kosinski M. What is AI security? | IBM. IBM - United States. URL: https://www.ibm.com/think/topics/ai-security.

6. Artificial Intelligence in Audit and Accounting: Development, Current Trends, Opportunities and Threats - Literature Review. IEEE Xplore. URL: https://ieeexplore.ieee.org/document/9057150

7. IBM leans into AI for managed security services. Network World. URL: https://www.networkworld.com/article/957376/ibm-leans-into-ai-for-managed-security-services.html.

Науковий керівник: ***Войтович Олеся Петрівна*** — канд. техн. наук, доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця,

e-mail: voytovych.op@gmail.com

Пилявець Ігор Юрійович — студент групи 1БС-23М, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця,

e-mail: igormorozov920@gmail.com.

Радченко Євгеній Валентинович — студент групи 1БС-23М, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця,

e-mail: jenya.radchenko@gmail.com.

Supervisor: ***Voytovych Olesya Petrovna*** — Cand. Sc., Associate Professor of Information Protection, Vinnytsia National Technical University, Vinnytsia, e-mail: voytovych.op@gmail.com

Pyliavets Ihor Y.— student of group 1BS-23M, faculty of information technologies and computer engineering, Vinnytsia National Technical University, email: igormorozov920@gmail.com.

Radchenko Yevhenii V.— student of group 1BS-23M, faculty of information technologies and computer engineering, Vinnytsia National Technical University, email: jenya.radchenko@gmail.com.