КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (31), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.31.1046
UDC 004.02

Oleksii Chalyi
Department of Cybersecurity and Information Protection
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine
ORCID: 0009-0006-3536-9715
oleksii.chalyi@knu.ua

Serhii Toliupa
Doctor of Technical Sciences, Professor
Professor of the Department of Cybersecurity and Information Protection
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine
ORCID: 0000-0002-1919-9174
serhii.toliupa@knu.ua

COMPARISON OF INTERNATIONAL AUDIT STANDARDS FOR INFORMATION SECURITY WITH AUTOMATION PERSPECTIVES

Abstract. This study presents a comparative analysis of three widely recognized audit-related international standards such as ISO 19011, ISO/IEC 27007, and ISA 200, aimed at identifying the most suitable methodological foundation for further research on the automation of audit management processes. The motivation for this work stems from the increasing complexity of audit activities in modern organizations and the growing need for structured, reproducible, and automatable audit procedures. A review of recent publications shows that comparative studies of audit standards remain limited, particularly in the context of information security and artificial intelligence, which underscores the relevance and originality of the present research. The evaluation methodology developed in this study incorporates a multi-criteria approach that considers academic visibility, general web presence, and the recency of each standard. Quantitative data from Google Scholar and Google Search were normalized using a dedicated formula to ensure comparability across different metrics. According to the calculated results, ISA 200 achieved the highest overall score due to its wide citation base and broad applicability across financial audit domains, while ISO/IEC 27007 received the lowest score because of its narrower scope and lower visibility. Despite ISA 200's quantitative advantage, the qualitative assessment demonstrates that ISO 19011 provides the most structured, universal, and adaptable audit framework, built around a clearly defined PDCA lifecycle. This structure is particularly advantageous for audit automation, as it offers a systematic sequence of actions that can be formalized and later integrated into AI-driven decision-making systems. Therefore, ISO 19011 is identified as the most appropriate standard for guiding future research on automated audit methodologies and for developing intelligent tools capable of supporting audit planning, execution, and follow-up activities.

Keywords: audit; cybersecurity; artificial intelligence; standard; iso 19011; comparison; information security;

INTRODUCTION

Audit is a critical mechanism for ensuring organizational transparency, accountability, and effective performance across both governmental and corporate environments. In the public sector, audits play a key role in reducing corruption, monitoring public financial management, and strengthening institutional accountability [1]. Prior research demonstrates that high-quality audits can significantly enhance government performance across multiple governance dimensions [2].

In the corporate sector, audits fulfill several essential functions, including fraud detection,

operational control, advisory support, and implementation of corporate governance principles [3]. Over time, internal audits have evolved from simple compliance checks to strategic management instruments that systematically evaluate organizational processes and protect financial interests [4]. The fundamental objective of any audit is to verify the correctness of internal processes and ensure compliance with organizational policies. Although the term "audit" is often associated primarily with financial auditing. For example, regulated by the Ukrainian Law "On the Audit of Financial Statements and Auditing Activities" [5] the methodological foundations of financial auditing provide valuable insights for other audit domains, including information security.

An information security audit is a comprehensive process aimed at evaluating an organization's information systems, identifying vulnerabilities, and ensuring the effectiveness of security controls. According to established information security management practices [6], such audits may be internal, conducted by the organization's security team or external, performed by independent auditors. The timing and frequency of these assessments should be defined in the organization's information security policy, and sudden or unannounced audits are generally discouraged to avoid unnecessary psychological pressure on employees. Information security audits are increasingly important, as modern organizations face rapidly growing technological risks, and systematic internal assessments increase the likelihood of adopting appropriate protective measures [7,8]. Their primary purpose is to safeguard organizational assets by examining security measures across administrative, physical, and technical domains [9,10]. Experts emphasize that security auditing should be treated as a continuous, iterative process rather than a one-time activity, balancing effective protection with system availability and user acceptance [11].

In recent years, the growing complexity of information systems and the rapid expansion of digital infrastructures have made manual audits increasingly resource-intensive and prone to human error [12]. Emerging AI-driven tools demonstrate strong potential to automate routine audit tasks, enhance detection accuracy, and support continuous monitoring, making the question of selecting a suitable audit standard for automation especially relevant.

Problem statement. Given the importance of information security auditing, the question of how to effectively manage this process becomes increasingly relevant. Multiple international standards govern audit management, including ISO 19011, ISO/IEC 27007 and ISA 200. However, despite the availability of multiple standards, there is limited comparative analysis focused specifically on their applicability for audit automation.This article aims to compare these standards, identify the most suitable one for automation, analyze their advantages and limitations, and propose a methodology for structured comparison of audit-related standards.

ANALYSIS OF RECENT RESEARCH AND PUBLICATIONS

Google Scholar and the Elicit tool were used to search for relevant research. The analysis showed that the number of studies comparing audit standards not only in information security but also in other scientific domains is limited. Therefore, only the most relevant and comprehensive publications were selected for this literature review.

Rosario et al. conducted a study on the formalization of the IT audit management process, aiming to analyze key frameworks, extract essential requirements, and use them to formalize IT audit management [13]. Their analysis focused on international standards such as ISO 38500, ITIL, COBIT, ISO/IEC 27001, ISO 19011, and ISO 31000. According to their findings, ISO 19011 provides the broadest coverage of organizational audit activities, while other standards

examined in their work offer similar levels of support for the audit process.

Lubenchenko et al., in their study on new standards of quality management in auditing, analyzed the implications of recently introduced quality management standards for audit firms, including ISQM 1 “Quality Management,” ISQM 2 “Engagement Quality Reviews,” and the revised ISA 220 “Quality Management for an Audit of Financial Statements” [14]. The authors outlined key components of these standards, such as risk assessment procedures, management and leadership requirements, ethical guidelines, client acceptance and engagement processes, resource management, communication, monitoring, and sanctions. Their conclusion emphasizes that the analyzed standards do not fully ensure internal firm control and still require significant manual adjustments.

Arief and Wahab, in their article on information technology audit for management evaluation, compared two frameworks for information security audit: COBIT 5 and the IT Security Standard for Information Technology Audit (ISO/IEC 1799) [15]. Using these frameworks, they evaluated the security posture of government institutions in Indonesia and identified only moderate maturity levels (e.g., 39% compliance with ISO/IEC 1799). Their findings confirm that standardized audit frameworks can effectively support security assessments at both organizational and state levels.

Griffiths, in his work on information audit and common methodologies, analyzed multiple issues in the current development of Information Audit (IA) and proposed a graphical representation of the IA landscape [16]. His article advocates for a more standardized and unified approach to information auditing, emphasizing the importance of consistent methods to improve the management and governance of organizational information assets. Griffiths concludes that the field must continue to evolve to address emerging audit and governance challenges.

Zakaira et al. presented a review of cybersecurity audit management and execution approaches, examining the main drivers behind cybersecurity audit research as well as existing models, scopes, strengths, and limitations [17]. Their study included an analysis of ISO/IEC 27001 and the NIST Cybersecurity Framework (NIST CSF). The authors concluded that cybersecurity audits can be significantly improved by addressing identified limitations and synthesizing best practices into a well-rounded approach for managing and executing cybersecurity audits.

PURPOSE OF THE RESEARCH

The analysis of related works has shown that most existing studies emphasize the importance of applying international standards for audit management, whether in information security or other fields [14–17]. These publications help identify the key standards that may be used for further comparison. However, the reviewed articles [14–17] do not provide a direct, systematic comparison of these standards. The only work that seeks to compare them [13] lacks a formalized methodology and relies primarily on expert judgment, which may reduce objectivity and reproducibility. This paper aims to address the limitations of previous research by providing a clear, structured methodology for comparing audit-related standards and presenting transparent, reproducible results.

METHODS

To properly evaluate and compare the selected standards, the following key elements

were considered:

- **Google Scholar Search Results** – the number of references to each standard in the Google Scholar academic database.
- **Google Search Results** – the number of references to each standard on the general web.
- **Year** – the release year of the most recent version of the standard.

These parameters were chosen because they jointly reflect academic relevance, practical visibility, and the recency of the standard, which are essential factors for assessing its applicability in modern audit processes.

Quantitative data were collected from Google Search and Google Scholar, two widely recognized indicators of web presence and academic visibility, following the methodology outlined in prior research [18]. Quotation marks (“ ”) were used to ensure exact phrase matching for each standard name [19]. Data collection was performed on October 7, 2025, using the search format: Standard name + “number” (e.g., ISO “19011”). Although search metrics do not measure audit quality directly, they serve as widely accepted proxies for academic influence and practical adoption

To normalize all results on a unified five-point scale, formula (1) was applied, following the approach used in earlier works [20]:

$$R = \frac{5 \times Rc}{Rb} \quad (1)$$

where

- **Rc** — the number of search results for the current standard.
- **Rb** — the highest number of results observed among all analyzed standards.
- **R** – result.

To evaluate the standards using all key elements simultaneously, the following formula (2) was applied:

$$R = \frac{\frac{GSc \times 5}{GSb} + \frac{Gc \times 5}{Gb}}{Yc - Ys} \quad (2)$$

where:

- **GSc** – number of Google Scholar results for the current standard.
- **GSb** – highest number of Google Scholar results among all tested standards.
- **Gc** – number of Google Search results for the current standard.
- **Gb** – highest number of Google Search results among all tested standards.
- **Yc** – current year.
- **Ys** – latest release year of the standard.
- **R** – result.

This methodology enables a consistent, reproducible, and quantifiable comparison of audit-related standards, ensuring that both academic relevance, web visibility, and standard recency are taken into account.

RESULTS

ISO 19011 “Guidelines for auditing management systems” (third edition, 2018) was developed by the International Organization for Standardization (ISO) [21]. As the core framework for conducting key audit stages, the standard applies the PDCA cycle (Plan–Do–Check–Act). The overall audit process is divided into two major phases: audit planning and audit conducting.

1. Audit planning phase — activities structured according to the PDCA cycle:

- **P**: Establishing audit objectives; determining and evaluating audit risks and opportunities; establishing the audit programme.
- **D**: Implementing the audit programme.
- **C**: Monitoring the audit programme.
- **A**: Reviewing and improving the audit programme.

2. Audit conducting phase — activities also aligned with PDCA:

- **P**: Initiating the audit and preparing audit activities.
- **D**: Conducting audit activities and preparing the audit report.
- **C**: Completing the audit.
- **A**: Conducting audit follow-up.

In addition to process structure, ISO 19011 provides detailed guidance on auditor selection, audit methods, and competence evaluation. The document outlines principles of auditing, requirements for managing an audit programme, and recommendations for conducting internal and external audits. The standard is applicable to any organization that needs to plan or perform audits of management systems or manage an audit programme.

Another international standard that addresses audit management is ISO/IEC 27007 “Guidelines for information security management systems auditing” (third edition, 2020), developed jointly by ISO and the International Electrotechnical Commission (IEC) [22]. Unlike ISO 19011, which covers auditing of management systems in general, ISO/IEC 27007 is specifically focused on the audit of Information Security Management Systems (ISMS).

The standard structures the audit process into three key components:

- Managing the audit programme.
- Conducting an audit.
- Competence and evaluation of auditors.

Similar to ISO 19011, ISO/IEC 27007 is also based on the PDCA lifecycle, and its stages largely align with the structure defined in ISO 19011. However, the standard extends this framework by contextualizing audit activities in the domain of information security and ISMS-specific requirements.

The document provides guidance applicable to organizations of all sizes and industries, covering ISMS audits of varying scope and complexity. It supports both large-scale audits performed by multi-person teams and smaller audits conducted by individual auditors. The guidance is intended to be adapted according to the scale, complexity, and objectives of the ISMS audit programme.

Another widely recognized framework relevant to audit management is ISA 200, issued by the International Auditing and Assurance Standards Board (IAASB) [23]. Unlike ISO 19011 and ISO/IEC 27007, which focus on management system audits, ISA 200 defines the general principles and responsibilities of auditors conducting financial audits, establishing the foundational requirements for performing audits in accordance with International Standards on Auditing.

ISA 200 outlines the auditor’s overall objectives, which include:

- Obtaining reasonable assurance that the financial statements as a whole are free from material misstatement, whether due to fraud or error.
- Reporting on the financial statements in accordance with the auditor’s findings.

The standard specifies a structured audit approach built around risk assessment, evidence collection, professional judgment, and application of ethical principles. While ISA 200 does not explicitly adopt the PDCA lifecycle, its methodology reflects a similar iterative

logic: planning the audit, performing audit procedures, evaluating results, and forming an opinion.

ISA 200 is applicable to organizations of all sizes and industries, defining a consistent global baseline for auditor competence, professional skepticism, documentation requirements, and audit quality. This standard establishes the fundamental objectives and principles governing the conduct of financial statement audits, serving as a cornerstone for ensuring reliability and transparency in audit practices.

Using the methodology described in the previous section, including formula (2), the evaluation results were calculated and summarized in Table 1.

Table 1.

Audit Standards Evaluation

Standard	GSc	Gc	GSc 5 point	Gc 5 point	Ys	R
ISO 19011	18700	1570000	0,091	0,888	2018	0,140
ISO/IEC 27007	1240	21500	0,006	0,012	2020	0,004
ISA 200	1030000	8840000	5,000	5,000	2015	0,526

Fig. 1 provides a visual representation of the obtained comparison results.

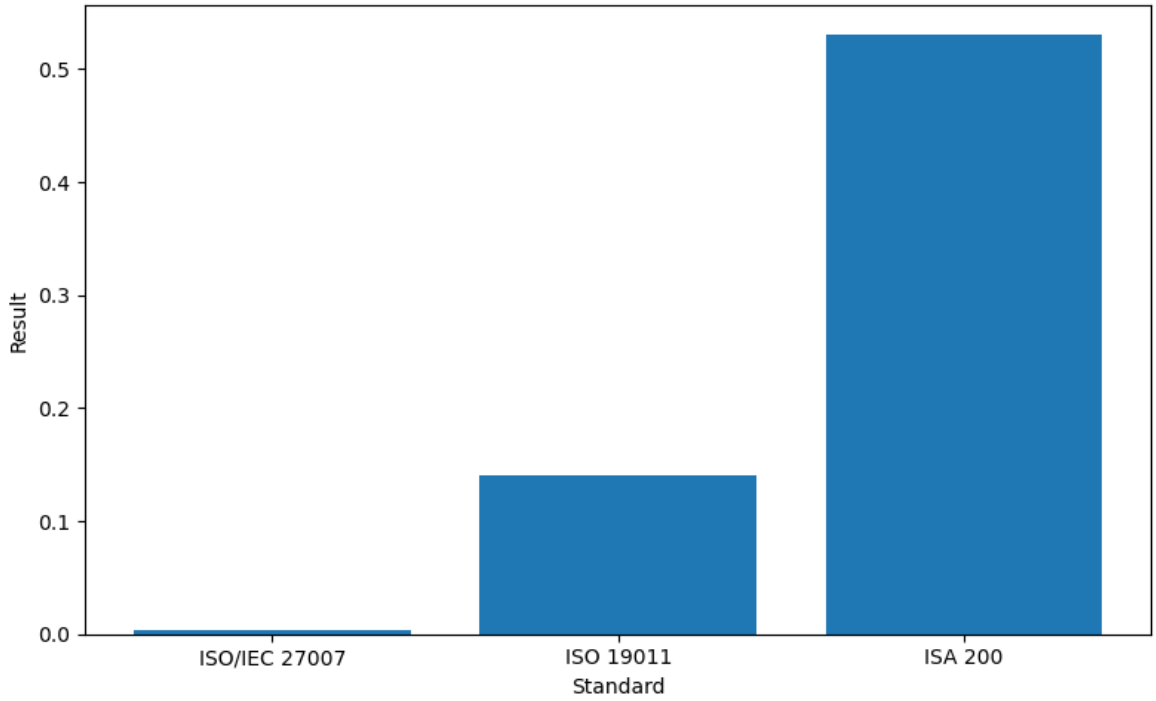

Fig. 1. Audit Standard Comparison Results

Based on the results presented in Table 1, ISA 200 achieved the highest score (0.526), followed by ISO 19011 (0.140) and ISO/IEC 27007 (0.004). Since the evaluation criteria rely largely on web and academic visibility, standards with broader applicability naturally obtain higher scores. However, in the context of information security audit automation, ISO 19011 and ISO/IEC 27007 remain more relevant, as both provide a structured PDCA-based

methodology. Such structured, cyclic processes are inherently more suitable for further automation using artificial intelligence.

CONCLUSIONS AND PROSPECTS FOR FURTHER RESEARCH

This study conducted a comparative evaluation of three international audit standards ISO 19011, ISO/IEC 27007, and ISA 200 with the aim of identifying the most suitable framework for the future development of automated audit methodologies. The analysis revealed that ISA 200 achieved the highest score in the quantitative assessment based on academic visibility, web presence, and standard recency. However, these metrics primarily reflect general popularity rather than applicability to information security audit automation.

A qualitative examination of the standards shows that ISO 19011 provides the most structured and universally adaptable audit methodology, particularly due to its clear PDCA-based lifecycle and comprehensive guidance on audit planning, execution, and auditor competence. ISO/IEC 27007 extends this structure into the information security domain but remains narrower in scope and less widely referenced. Therefore, despite ISA 200's prominence in quantitative indicators, ISO 19011 is identified as the most appropriate foundation for further research, especially in the context of designing audit processes that can be automated using artificial intelligence.

Future work will focus on:

- developing an AI-driven methodology that applies ISO 19011's PDCA-based structure to automate audit planning, evidence collection, and reporting.
- designing a standardized audit knowledge base that can serve as input for machine learning models.
- validating the proposed automation framework on real-world audit cases.

This study provides a structured foundation for advancing research in automated audit processes and highlights ISO 19011 as a key enabler for future AI-supported audit methodologies. Additionally, the findings provide a reproducible methodological basis for future comparative studies of audit and cybersecurity standards.

REFERENCES

1. Ionescu, L. (2014). THE ROLE OF GOVERNMENT AUDITING IN CURBING CORRUPTION. *Economics, Management, and Financial Markets*, 9, 122-127.
2. Riahi-Belkaoui, A. (2004). Are You Being Fooled? Audit Quality and Quality of Government. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.485764
3. ABBAS, Z., & BENAOUIDA, N. (2022). Internal auditing as one of the most important internal mechanisms for embodying the principles of Corporate Governance. *Advanced Research in Economics and Business Strategy Journal*, *3*(1), 5–36. https://doi.org/10.52919/arebus.v3i1.23
4. Lozano, G., & Carina, L. (2014). La importancia de las auditorías internas y externas dentro de las organizaciones.
5. Verkhovna Rada of Ukraine, On the Audit of Financial Statements and Auditing Activities, Law of Ukraine No. 2258-VIII, 2017. URL: https://zakon.rada.gov.ua/laws/show/2258-19#Text
6. Toliupa, S., V., Politanskyi, L., F., Politanskyi, R., L., & Lesinskyi, V., V. Information Security Management: Textbook, *Yuriy Fedkovych Chernivtsi National University*, Chernivtsi, Ukraine, 2021, 540 p.
7. Chalyi, O., & Stopochkina, I. (2024). INFORMATION RETRIEVAL AND DEANONYMIZATION IN THE TASKS OF EARLY DETECTION OF POTENTIAL ATTACKS ON CRITICAL INFRASTRUCTURE. *Cybersecurity Education Science Technique*, *2*(26), 305–322. https://doi.org/10.28925/2663-4023.2024.26.694

8. Suduc, A., Bîzoi, M., Filip, F.G., & Academy-INCE, R. (2010). Audit for Information Systems Security. *Informatică economică*, 14, 43-48.
9. Kozhakhmet, K.T., Bortsova, G.K., Inoue, A., & Atymtayeva, L.B. (2012). Expert System for Security Audit Using Fuzzy Logic. Midwest Artificial Intelligence and Cognitive Science Conference.
10. Chalyi, O. (2025). Assessing Wi-Fi Security Protocols: A Study of Dictionary Attack Performance. *Baltic Journal of Modern Computing*, *13*(3). https://doi.org/10.22364/bjmc.2025.13.3.03
11. Lo, E. C., & Marchand, M. (n.d.). Security audit: a case study [information systems]. *Canadian Conference on Electrical and Computer Engineering 2004 (IEEE Cat. No.04CH37513)*. https://doi.org/10.1109/ccece.2004.1344989
12. Chalyi, O. (2024). An Evaluation of General-Purpose AI Chatbots: A Comprehensive Comparative Analysis. *Infoscience Trends*. *1(1)*, 52–66. https://doi.org/10.61186/ist.202401.01.07
13. Rosário, T., Pereira, R., & da Silva, M. M. (2012, September 1). *Formalization of the IT Audit Management Process*. IEEE Xplore. https://doi.org/10.1109/EDOCW.2012.11
14. Lubenchenko, O. E., Shulha, S. V., & Korinko, M. D. (2022). New Standards of Quality Management in Audit. The Risk-Based Approach. *Statistics of Ukraine*, *96*(1), 117–126. https://doi.org/10.31767/su.1(96)2022.01.11
15. Assaf Arief, & Ayub, H. (2016). *Information technology audit for management evaluation using COBIT and IT security (Case study on Dishubkominfo of North Maluku Provincial Government, Indonesia)*. https://doi.org/10.1109/icitacee.2016.7892477
16. Griffiths, P. (2012). Information Audit: Towards common standards and methodology. *Business Information Review*, *29*(1), 39–51. https://doi.org/10.1177/0266382112436791
17. Zakaria, K., N., Othman, H., S., &Zainal, A. (2019). *Review of Cybersecurity Audit Management and Execution Approaches*. https://doi.org/10.1109/icriis48246.2019.9073641
18. Chalyi, O., Driaunys, K., & Rudžionis, V. (2025). Assessing Browser Security: A Detailed Study Based on CVE Metrics. *Future Internet*, *17*(3), 104–104. https://doi.org/10.3390/fi17030104
19. Reuben-Owoh, B., & Haig, E. (2025). A Systematic Review of Voluntary Cybersecurity Standards and Frameworks. *International Journal of Information Security*, *24*(5). https://doi.org/10.1007/s10207-025-01121-0
20. Chalyi, O., & Kolomytsev, M. (2023). Comparison of Tools for Web-Application Brute Forcing. *Theoretical and Applied Cybersecurity*, *4*(1). https://doi.org/10.20535/tacs.2664-29132022.1.274117
21. International Organization for Standardization. (2018). *ISO 19011:2018 — Guidelines for auditing management systems*. ISO.
22. International Organization for Standardization & International Electrotechnical Commission. (2020). *ISO/IEC 27007:2020 — Guidelines for information security management systems auditing*. ISO.
23. International Auditing and Assurance Standards Board. (2009). *ISA 200: Overall objectives of the independent auditor and the conduct of an audit in accordance with International Standards on Auditing*. IFAC.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (31), 2025
ISSN 2663 - 4023

Чалий Олексій Віталійович
Кафедра кібербезпеки та захисту інформації
Київський національний університет імені Тараса Шевченка, Київ, Україна
ORCID: 0009-0006-3536-9715
oleksii.chalyi@knu.ua

Толюпа Сергій Васильович
доктор технічних наук, професор,
професор кафедри кібербезпеки та захисту інформації
Київський національний університет імені Тараса Шевченка, Київ, Україна
ORCID: 0000-0002-1919-9174
serhii.toliupa@knu.ua

ПОРІВНЯННЯ МІЖНАРОДНИХ СТАНДАРТІВ АУДИТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ З ПЕРСПЕКТИВОЮ АВТОМАТИЗАЦІЇ

Анотація. Дане дослідження представляє порівняльний аналіз трьох широко визнаних міжнародних стандартів, пов'язаних з аудитом, таких як ISO 19011, ISO/IEC 27007 та ISA 200, з метою визначення найбільш відповідної методологічної основи для подальших досліджень щодо автоматизації процесів управління аудитом. Мотивація цієї роботи зумовлена зростаючою складністю аудиторської діяльності в сучасних організаціях та зростаючою потребою у структурованих, відтворюваних і таких, що підлягають автоматизації, аудиторських процедурах. Огляд сучасних публікацій показує, що порівняльних досліджень стандартів аудиту все ще обмаль, особливо в контексті інформаційної безпеки та штучного інтелекту, що підкреслює актуальність і новизну даної роботи. Розроблена в дослідженні методологія оцінювання базується на багатокритеріальному підході, який враховує академічну видимість, загальну веб-присутність та актуальність кожного стандарту. Кількісні дані з Google Scholar та Google Search було нормалізовано за допомогою спеціальної формули для забезпечення коректної порівнюваності між показниками. Відповідно до отриманих результатів, ISA 200 посів найвищу позицію завдяки широкій цитованості та широкій застосовності у фінансовому аудиті, тоді як ISO/IEC 27007 отримав найнижчу оцінку через вузькість сфери застосування та нижчу загальну видимість. Попри кількісну перевагу ISA 200, якісний аналіз показує, що ISO 19011 забезпечує найбільш структуровану, універсальну та адаптивну основу для проведення аудиту, побудовану навколо чітко визначеного PDCA-циклу. Така структура є особливо сприятливою для автоматизації аудиторських процесів, оскільки пропонує системну послідовність дій, яку можна формалізувати та інтегрувати у системи підтримки прийняття рішень на основі штучного інтелекту. Тому ISO 19011 визначено як найбільш відповідний стандарт для подальших досліджень у сфері автоматизованих аудиторських методологій і для розробки інтелектуальних інструментів, здатних підтримувати планування аудиту, виконання перевірок та подальші коригувальні дії.

Ключові слова: аудит; кібербезпека; штучний інтелект; стандарти; iso 19011; порівняння; інформаційна безпека;

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Ionescu, L. (2014). THE ROLE OF GOVERNMENT AUDITING IN CURBING CORRUPTION. *Economics, Management, and Financial Markets*, 9, 122-127.
2. Riahi-Belkaoui, A. (2004). Are You Being Fooled? Audit Quality and Quality of Government. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.485764
3. ABBAS, Z., & BENAOUIDA, N. (2022). Internal auditing as one of the most important internal mechanisms for embodying the principles of Corporate Governance. *Advanced Research in Economics and Business Strategy Journal*, *3*(1), 5–36. https://doi.org/10.52919/arebus.v3i1.23
4. Lozano, G., & Carina, L. (2014). La importancia de las auditorías internas y externas dentro de las organizaciones.

5. Verkhovna Rada of Ukraine, On the Audit of Financial Statements and Auditing Activities, Law of Ukraine No. 2258-VIII, 2017. URL: https://zakon.rada.gov.ua/laws/show/2258-19#Text
6. Toliupa, S.,V., Politanskyi, L.,F., Politanskyi, R.,L., & Lesinskyi, V.,V. Information Security Management: Textbook, *Yuriy Fedkovych Chernivtsi National University*, Chernivtsi, Ukraine, 2021, 540 p.
7. Chalyi, O., & Stopochkina, I. (2024). INFORMATION RETRIEVAL AND DEANONYMIZATION IN THE TASKS OF EARLY DETECTION OF POTENTIAL ATTACKS ON CRITICAL INFRASTRUCTURE. *Cybersecurity Education Science Technique*, *2*(26), 305–322. https://doi.org/10.28925/2663-4023.2024.26.694
8. Suduc, A., Bîzoi, M., Filip, F.G., & Academy-INCE, R. (2010). Audit for Information Systems Security. *Informatică economică*, 14, 43-48.
9. Kozhakhmet, K.T., Bortsova, G.K., Inoue, A., & Atymtayeva, L.B. (2012). Expert System for Security Audit Using Fuzzy Logic. Midwest Artificial Intelligence and Cognitive Science Conference.
10. Chalyi, O. (2025). Assessing Wi-Fi Security Protocols: A Study of Dictionary Attack Performance. *Baltic Journal of Modern Computing*, *13*(3). https://doi.org/10.22364/bjmc.2025.13.3.03
11. Lo, E. C., & Marchand, M. (n.d.). Security audit: a case study [information systems]. *Canadian Conference on Electrical and Computer Engineering 2004 (IEEE Cat. No.04CH37513)*. https://doi.org/10.1109/ccece.2004.1344989
12. Chalyi, O. (2024). An Evaluation of General-Purpose AI Chatbots: A Comprehensive Comparative Analysis. *Infoscience Trends*. *1(1)*, 52–66. https://doi.org/10.61186/ist.202401.01.07
13. Rosário, T., Pereira, R., & da Silva, M. M. (2012, September 1). *Formalization of the IT Audit Management Process*. IEEE Xplore. https://doi.org/10.1109/EDOCW.2012.11
14. Lubenchenko, O. E., Shulha, S. V., & Korinko, M. D. (2022). New Standards of Quality Management in Audit. The Risk-Based Approach. *Statistics of Ukraine*, *96*(1), 117–126. https://doi.org/10.31767/su.1(96)2022.01.11
15. Assaf Arief, & Ayub, H. (2016). *Information technology audit for management evaluation using COBIT and IT security (Case study on Dishubkominfo of North Maluku Provincial Government, Indonesia)*. https://doi.org/10.1109/icitacee.2016.7892477
16. Griffiths, P. (2012). Information Audit: Towards common standards and methodology. *Business Information Review*, *29*(1), 39–51. https://doi.org/10.1177/0266382112436791
17. Zakaria, K., N., Othman, H., S., &Zainal, A. (2019). *Review of Cybersecurity Audit Management and Execution Approaches*. https://doi.org/10.1109/icriis48246.2019.9073641
18. Chalyi, O., Driaunys, K., & Rudžionis, V. (2025). Assessing Browser Security: A Detailed Study Based on CVE Metrics. *Future Internet*, *17*(3), 104–104. https://doi.org/10.3390/fi17030104
19. Reuben-Owoh, B., & Haig, E. (2025). A Systematic Review of Voluntary Cybersecurity Standards and Frameworks. *International Journal of Information Security*, *24*(5). https://doi.org/10.1007/s10207-025-01121-0
20. Chalyi, O., & Kolomytsev, M. (2023). Comparison of Tools for Web-Application Brute Forcing. *Theoretical and Applied Cybersecurity*, *4*(1). https://doi.org/10.20535/tacs.2664-29132022.1.274117
21. International Organization for Standardization. (2018). *ISO 19011:2018 — Guidelines for auditing management systems*. ISO.
22. International Organization for Standardization & International Electrotechnical Commission. (2020). *ISO/IEC 27007:2020 — Guidelines for information security management systems auditing*. ISO.
23. International Auditing and Assurance Standards Board. (2009). *ISA 200: Overall objectives of the independent auditor and the conduct of an audit in accordance with International Standards on Auditing*. IFAC.