УДК: 657.6:004.7:330.341.1
https://doi.org/10.32342/3041-2137-2026-2-65-10

Artem Basin,
Postgraduate Student (PhD) of the Department of Audit,
Kyiv National Economic University named after Vadym Hetman, Kyiv (Ukraine)
https://orcid.org/0009-0003-4579-3315

Olena Petryk,
Doctor of Sciences (Economics), Professor, Head of the Department of Audit,
Kyiv National Economic University named after Vadym Hetman, Kyiv (Ukraine)
https://orcid.org/0000-0003-1881-9412

Yuliia Slobodianyk,
Doctor of Sciences (Economics), Professor, Professor of the Department of Audit,
Kyiv National Economic University named after Vadym Hetman, Kyiv (Ukraine)
https://orcid.org/0000-0002-5838-2342

PECULIARITIES OF DIGITAL AUDIT IN THE IT INDUSTRY: METHODOLOGICAL AND PRACTICAL ASPECTS

This article examines the theoretical and practical aspects of Digital Audit in the IT industry, highlighting the transformation of auditing practices under digitalization. It demonstrates that enhancing audit efficiency through digitalization demands new approaches, tools, methods, and auditor upskilling. Multidimensional taxonomic models of Digital Audit and their specific implementation in IT companies are characterized. The Digital Audit toolkit is defined, considering IT industry functional characteristics, and its development prospects are substantiated through the integration of artificial intelligence and blockchain. Conclusions are drawn and strategic recommendations are proposed for IT industry auditors regarding Digital Audit implementation, considering Ukraine's integration into the European economic space.

The study's relevance stems from digital audit's role in optimizing business processes and ensuring investor confidence. AI integration is crucial for enhancing audit accuracy and timeliness, leading to Digital Audit, highly pertinent to the IT sector.

The implementation of advanced technologies (AI, cloud computing, blockchain, automation) not only accelerates audit but also redefines auditor skill requirements, demanding technological fluency and critical thinking. This introduces risks like data governance and algorithmic bias. The research emphasizes balancing human expertise and technology for effective oversight. Digital Audit in the IT industry is a multidimensional process covering technical, operational, and ethical aspects. Its strategic importance for sustainable IT company development and maintaining digital economy trust is significant. During wartime, digital audit aids in protecting critical infrastructure, identifying vulnerabilities, increasing transparency in government and defense IT projects, and ensuring international standard compliance. It is a vital mechanism for overseeing post-war recovery. Challenges include personnel shortages, lack of unified methodologies, high costs, and cyber risks. Continuous training and investment in advanced technologies are necessary for enhanced effectiveness.

Keywords: Digital audit, IT industry, cybersecurity, artificial intelligence, blockchain, DevOps, cloud infrastructure, regulatory compliance, data governance, sustainable development

JEL classification: ***D83, L86, M15, M45***

У статті досліджено теоретичні та практичні аспекти цифрового аудиту в ІТ-індустрії, підкреслюючи трансформацію аудиторської практики в умовах цифровізації. Показано, що підвищення ефективності аудиту через цифровізацію вимагає нових підходів, інструментів, методів та підвищення кваліфікації аудиторів. Охарактеризовано багатовимірні таксономічні моделі цифрового аудиту та специфіку їх впровадження в ІТ-компаніях. Визначено інструментарій цифрового аудиту з урахуванням функціональних особливостей ІТ-індустрії та обґрунтовано перспективи його розвитку завдяки інтеграції штучного інтелекту та блокчейну. Сформульовано висновки та запропоновано стратегічні рекомендації щодо впровадження цифрового аудиту для аудиторів ІТ-індустрії, враховуючи інтеграцію України в європейський економічний простір.

Актуальність дослідження цифрового аудиту в ІТ-індустрії зумовлена його роллю в оптимізації бізнес-процесів та забезпеченні довіри інвесторів. Інтеграція штучного інтелекту є ключовою для підвищення точності та оперативності аудитів, що призвело до появи окремої форми – Цифрового аудиту, особливо актуального в ІТ-галузі.

Впровадження передових технологій (ШІ, хмарні обчислення, блокчейн, автоматизація) не лише прискорює аудит, а й змінює вимоги до навичок аудиторів, вимагаючи технологічної грамотності та критичного мислення. Це створює ризики, зокрема щодо управління даними та алгоритмічної упередженості. Дослідження підкреслює необхідність балансу між людським досвідом та технологіями для ефективного нагляду. Цифровий аудит у ІТ-індустрії є багатовимірним процесом, що охоплює технічні, операційні та етичні аспекти. Його стратегічне значення для сталого розвитку ІТ-компаній та підтримки довіри до цифрової економіки є значним. Під час війни цифровий аудит допомагає захистити критичну інфраструктуру, виявляти вразливості, підвищувати прозорість у державних та оборонних ІТ-проектах, а також забезпечувати відповідність міжнародним стандартам. Він є важливим механізмом для нагляду за повоєнним відновленням. Проте існують виклики: дефіцит кадрів, відсутність єдиних методологій, високі витрати та кіберризики. Для підвищення ефективності необхідні безперервне навчання та інвестиції в передові технології.

Ключові слова: цифровий аудит, ІТ-галузь, кібербезпека, штучний інтелект, блокчейн, DevOps, хмарна інфраструктура, дотримання нормативних вимог, управління даними, сталий розвиток

JEL classification: ***D83, L86, M15, M45***

Introduction. The paradigmatic transformation of economic processes in the context of the global digital revolution necessitates a reconceptualization of traditional methodological approaches to auditing, particularly within the IT industry. The functioning of the IT sector as a leading component of Ukraine's economic system has persisted despite the prolonged military conflict and mobilization pressures. This sector not only provides significant export potential but also plays a decisive role in the country's digital transformation, the development of innovative solutions for enhancing resource management efficiency, and ensuring resilience and infrastructure reconstruction.

Comprehensive digitalization of the economy and society, a sufficiently strong human capital base, and a well-developed system of specialist training have facilitated the formation and advancement of a robust information technology industry in Ukraine. As of April 2025, the industry employs approximately 300,000 professionals [8], while revenues from the export of IT products and services reached USD 6.45 billion in 2024 [16]. According to the Unified State Register of Legal Entities and Individual Entrepreneurs, as of February 24, 2025, there were 262,093 active sole proprietors registered under IT-related activity codes in Ukraine [8].

Problem Statement. The current economic landscape is marked by an exceptionally rapid pace of digitalization, which is increasingly seen as "a holistic approach to thinking that encompasses all processes" (Astakhova, 2007) [5, p.319]. This has led to a sharply rising demand for continuous monitoring and evaluation of economic entities in terms of their efficiency and competitiveness.

Audit, both internal and external, plays a crucial role in optimizing business processes, improving management efficiency, and ensuring investor confidence in financial reporting. The integration of Artificial Intelligence (AI) into these frameworks represents a pivotal change, enhancing the ability to conduct thorough audits with greater accuracy and real-time insights [18, pp. 4-6]. In the context of digitalization, auditing is undergoing substantial changes, with transformations in its approaches, methods, and practices. This evolution has given rise to a distinct form of auditing – Digital Audit, which is particularly relevant in the IT industry due to its specific characteristics.

All of the above underscores the relevance and practical importance of investigating the current state and development prospects of Digital Audit, with a focus on its specific features and methodological and practical dimensions in the IT industry.

Literature Review. Auditing continues to be the focus of considerable attention among both domestic and international scholars in the fields of accounting theory and practice. However, Digital Audit as a distinct area of accounting and control has received substantial academic attention only within the last decade. Specifically, the implementation of digital technologies in accounting and auditing, the conduct of audits amid global crises, and the transformation of audit activity as a driver of sustainable economic development have been explored in the works of S. Korol [12], M. Nezhyva [17], V. Minyaylo [17] and I. Kryukova [13].

The impact of digital auditing on corporate governance mechanisms has been examined in the studies of international researchers such as R. Manita, N. Elommal, P. Baudier, and L. Hikkerova (2020) [15, pp. 3-5]. Methods for fraud detection in digital environments are thoroughly discussed in the work of P.S. Tjeng and R. Nopianti (2020) [21, p. 47-50]. Changes in the functional capabilities of internal audit under digital transformation have been analyzed by P. Lois, G. Drogalas, A. Karagiorgos, and K. Tsikalakis (2020) [14, p. 208].

In recent years, the digital technology paradigm has undergone significant shifts, particularly in accounting and auditing. These areas are experiencing the active integration of artificial intelligence, cloud computing, big data, blockchain, and comprehensive process automation. As emphasized by M.G. Alles (2015), the implementation of these advanced technologies goes far beyond accelerating audit procedures; it also redefines the skill set required of audit professionals —necessitating technological fluency and enhanced critical thinking [2, pp. 444–446]. However, this also brings forth certain risks and caveats. M. Power (1997) highlights that audit automation raises critical concerns about data governance, particularly with respect to safeguarding confidential information and managing algorithmic bias [19, pp. 27-29]. A.A. Arens, R.J. Elder, & M.S. Beasley (2020) stress the importance of maintaining a balance between human expertise and high-tech interventions to ensure effective oversight and prevent excessive dependence on digital tools [4, pp. 400-405]. Moreover, as highlighted in recent studies, the integration of social factors significantly influences the occurrence of fraudulent behavior in digital environments, necessitating comprehensive audit strategies that address both technological and human elements in organizations [1, pp. 29-31, 53-54, 100-102]. This dual focus on technical proficiency and social governance is critical in mitigating risks and ensuring organizational resilience in the face of evolving digital landscapes [14, p. 208]. Deloitte (2022), in its *Transparency Report*, notes that modern audit firms are expected not only to verify and oversee financial performance but also to contribute to governance improvements and risk management practices [7, pp. 6-7]. The role of auditors in the new digital environment requires a transformation of traditional auditing approaches, along with greater transparency and accountability [20].

Materials and Methods. This study is based on a conceptual and comparative analysis of Digital Audit in the IT industry. The methodological framework integrates interdisciplinary approaches from audit

theory, information systems, cybersecurity governance, and digital transformation management. The research methodology includes four key components:

1. Epistemological justification: The foundation of the study lies in understanding Digital Audit as a system grounded in empirical (data-based), rationalist (standard-based), constructivist (contextual), and pragmatic (problem-solving) knowledge systems. This approach enables a comprehensive interpretation of how Digital Audit functions within complex IT environments.

2. Analytical techniques: A combination of deductive reasoning, expert-based generalization, and taxonomic modeling was applied to structure the audit process into key domains (technological, legal, ethical, operational, and economic). Methodological triangulation ensures the validity of synthesized models and classifications.

3. Source basis and regulatory frameworks: The study relies on international and national standards, such as ISO/IEC 27001, NIST frameworks, OWASP, GDPR, and the EU AI Act, which served as references for validating best practices in IT audit. Tools and platforms mentioned (e.g., SonarQube, Fortify, Tableau, Power BI) illustrate current technological implementations.

4. Approach to data synthesis: Although the study is theoretical, its conclusions are drawn from the synthesis of documented practices, academic literature, expert reports, and policy papers on digital audit applications in IT enterprises, particularly under war-time and post-crisis conditions in Ukraine.

The overall methodology is designed to be reproducible for further research in auditing practices, digital governance, and regulatory alignment within digitally transforming economies.

Results and Discussion. In the context of digital transformation, auditing requires fundamentally new approaches that involve a shift from traditional document verification to the comprehensive analysis of digital assets and business processes. The IT industry, being one of the most dynamic and knowledge-intensive sectors of the economy, necessitates the development of a specialized methodological toolkit for evaluation and verification, tailored to its specificities and the transformational potential of emerging technologies. Of particular importance is the formation of a systemic approach to auditing that encompasses technical, managerial, and ethical aspects of digital processes.

The issue of audit development under conditions of intensive digitalization has been the subject of research by many scholars. D. Ben Ahmed's research demonstrates that artificial intelligence minimises information asymmetry and significantly enhances the transparency of financial data. This frees auditing from routine verification, transforming it into a proactive mechanism for strategic decision-making, which provides companies with a sustainable competitive advantage in a dynamic market [6, pp. 3–4]. R.L. Us (2022) conducted an in-depth study of the preconditions for the emergence and subsequent evolution of the concept of IT audit as an innovative branch of organizational auditing, analyzing its ontological foundations and practical implementation within the economic management system [22, pp. 140–142].

A definition provided by Eamonn O'Raghallaigh in his article for Digital Strategy Consultants aptly characterizes Digital Audit as: "a comprehensive review of your organization's digital assets and their performance in the context of business goals and profitability. It helps identify areas of success, gaps, quick wins, and areas that require improvement" [9, p. 1].

Digital Audit serves as a key instrument that integrates data analysis, risk assessment, and transparency assurance to achieve the Sustainable Development Goals (SDGs). This tool is particularly relevant for Ukraine, which actively attracts international funding, while investors and partners demand openness, reliable control mechanisms, and efficient use of resources. Digital Audit contributes to establishing the necessary trust, thereby accelerating processes of recovery and sustainable development. This role of Digital

Audit as a tool of trust and transparency not only underscores its practical value but also opens new perspectives for the advancement of its theoretical foundations.

Digital Audit, in this regard, can be conceptualized as a complex system built upon interconnections between sources of knowledge, evaluation tools, and the environment for implementing digital solutions.

Firstly, it is grounded in epistemological foundations – methods of understanding and analyzing information processes. In the context of the IT industry, these foundations include an empirical approach, which relies on data from digital systems (logs, metrics, configurations), and a rationalist approach involving the application of standards (such as ISO 27001, NIST) and logical reasoning for assessing risks and compliance. Additionally, the epistemology of Digital Audit embraces a constructivist perspective, which acknowledges the uniqueness of each IT system and its operational context, as well as a pragmatic approach that values knowledge based on its problem-solving capacity, such as enhancing cybersecurity or optimizing resource usage. Thus, the epistemological base of Digital Audit integrates interdisciplinary knowledge with analytical technologies.

Secondly, Digital Audit entails verification and validation methods for digital transformations, aiming to ensure their reliability and effectiveness. This includes cognitive mapping—the visualization and structuring of information processes to better understand complex systems, which is particularly important in IT, where networks, databases, and software form multilayered infrastructures. Furthermore, it involves risk scenario modeling and forecasting the impacts of digital changes using historical data and trend analysis.

Thirdly, it includes analytical diagnostics, enabling the detection of hidden information risks, such as code vulnerabilities or suboptimal configurations. AI-driven diagnostic tools (e.g., predictive analytics) make it possible not only to respond to incidents but also to proactively prevent them. These aspects open new avenues for analytics and risk management in the digital domain, ensuring not only technical reliability but also strategic value for organizations and countries aiming for sustainable development in a digitalized world.

In the IT industry, Digital Audit transcends traditional financial reporting analysis by encompassing a comprehensive assessment of business processes specific to the sector. Therefore, Digital Audit in IT integrates technical, operational, and ethical dimensions aimed at ensuring the reliability, security, and ethical integrity of digital systems. The adoption of artificial intelligence (AI) has been particularly pivotal, as it enables auditors to automate routine tasks, analyze large datasets, and detect anomalies with remarkable precision, thereby enhancing the overall efficiency and quality of audits (Pinto, 2024). Concurrently, the industry has witnessed a shift from traditional, document-based auditing to more dynamic, transaction-based approaches that facilitate real-time monitoring and proactive risk management [3, p. 3–5, 7]. Research by Kokina et al. (2017) supports the modernization of audit methods through the use of analytics, AI, and digital technologies, emphasizing their role in transforming audit practices (Kokina, 2017) [11, pp. 115-117]. These methodologies emphasize the importance of adaptability and strategic foresight within the realm of digital audits, ensuring compliance and reliability in an increasingly digital economy. This multidimensional approach addresses the unique challenges of the IT environment and considers the sector's dependency on complex technological ecosystems.

The technological dimension of Digital Audit provides a systematic analysis of core infrastructure components, such as software, databases, cloud services, application programming interfaces (APIs), and digital platforms. This process assesses the performance, scalability, and interoperability of these components to ensure alignment with organizational objectives and industry standards (e.g., ISO/IEC 27001, NIST Cybersecurity

Framework). For instance, auditors review cloud infrastructure configurations to identify inefficiencies or non-compliance with best practices, such as those outlined by the Cloud Security Alliance (CSA). Similarly, API audits focus on security, documentation, and compliance with standards like OpenAPI. By analyzing these elements, Digital Audit strengthens the reliability and optimization of an IT system's technological foundation for both current and future needs.

For product-oriented IT companies, code auditing is a critical component of Digital Audit, aimed at identifying vulnerabilities and ensuring software quality. This process includes both static and dynamic analysis of source code to detect issues such as SQL injection flaws or authentication breaches. Static analysis tools like SonarQube and Fortify, combined with manual code reviews, enable auditors to deeply evaluate the codebase for compliance with secure coding practices recommended by the Software Engineering Institute (SEI). Such an approach enhances the overall quality of software by enabling the early identification and resolution of critical flaws that may compromise system security, erode user trust, or damage the organization's reputation.

Another vital aspect of Digital Audit for both product and service-based IT companies is the assessment of cloud infrastructure (e.g., AWS, Microsoft Azure, Google Cloud) and database management systems (including SQL and NoSQL solutions) in terms of their efficiency, security, and cost-effectiveness. This type of audit ensures compliance with regulatory and security standards (such as GDPR or CCPA) while optimizing expenditures on computational resources, thereby improving the overall performance and resilience of the IT architecture.

With the widespread adoption of artificial intelligence (AI) in IT products and services, ethical auditing has emerged as a key dimension of modern Digital Audit. This type of audit evaluates AI systems with respect to bias, fairness, transparency, and potential social risks. In this context, auditors follow international guidelines such as the IEEE Ethically Aligned Design or the EU AI Act to identify discriminatory behavior in algorithms, violations of ethical principles, or opaque decision-making mechanisms. For example, ethical audits may scrutinize training datasets for representativeness or assess the transparency of AI decision logic. Addressing such issues reduces deployment-related risks, fosters stakeholder trust, and ensures alignment with global ethical standards.

Overall, Digital Audit in the IT industry has evolved into a multidimensional instrument that transcends traditional financial auditing. It is tailored to the specific technological, security, and ethical challenges of the digital economy. A comprehensive approach — encompassing infrastructure, source code, cloud services, databases, and AI-based systems — provides an integrated assessment of the security, efficiency, and ethical integrity of IT organizations. In doing so, Digital Audit strengthens operational resilience while aligning with broader strategic goals such as transparency, accountability, and sustainable development in the context of digital transformation.

For a deeper understanding of the role of Digital Audit in the IT industry, it is necessary to analyze its core dimensions in detail. This transition from a general overview to a structured analysis allows for a systematic classification of Digital Audit's components, highlighting their contributions to the technical, operational, and ethical sustainability of information and communication systems. Within this study, particular attention is devoted to the multidimensional framework of Digital Audit, encompassing technological, process, legal, ethical, and economic dimensions of digital systems. Such a typology not only facilitates the classification of major audit areas but also links them to relevant methodologies, challenges, and epistemological foundations that shape the approaches to their research and implementation.

Table 1 presents a structured overview of the key aspects of Digital Audit in the IT industry. It outlines the primary audit dimensions, their objectives, methods, regulatory frameworks, typical challenges, and epistemological underpinnings, which together form the scientific basis of modern Digital Audit.

Table 1

Key Aspects of Digital Audit in the IT Industry*

Aspect	Description	Key Objectives	Methods and Tools	Regulatory Frameworks and Standards
Technological Audit	Assessment of IT infrastructure (software, cloud services, APIs, databases)	Ensure performance, security, scalability	Static and dynamic analysis, monitoring, testing	ISO/IEC 27001, NIST, OpenAPI, GDPR
Source Code Audit	Evaluation of code quality and security	Detect vulnerabilities, ensure software stability	SAST (SonarQube), DAST (Burp Suite), manual code review	OWASP Top 10, SEI CERT
AI Ethics Audit	Evaluation of AI systems for bias, transparency, and ethical compliance	Mitigate ethical risks, foster trust in AI	Data analysis, SHAP, LIME, model auditing	IEEE Ethically Aligned Design, EU AI Act
DevSecOps Process Audit	Security analysis within CI/CD pipelines	Embed security across all development stages	Jenkins, GitLab CI/CD, automated testing	OWASP DevSecOps, NIST SP 800-53
Cybersecurity and Incident Audit	Evaluation of cybersecurity and incident readiness	Resilience to attacks, rapid recovery	Penetration testing, SIEM (Splunk, QRadar)	ISO/IEC 27035, MITRE ATT&CK
Regulatory Compliance Audit	Verification of legal compliance in IT operations	Legal compliance, reduced regulatory risks	Policy analysis, compliance audit	GDPR, NIS2, Ukrainian Law "On Information Protection"
IP and Intangible Assets Audit	Assessment of compliance with IP, licenses, and patents	Asset protection, dispute risk mitigation	License audit, contract/legal review	WIPO, TRIPS, Ukrainian Law "On Copyright and Related Rights"
Project and Portfolio Management Audit	Evaluation of IT project and portfolio performance	Increase ROI and efficiency	PM audit, KPI analysis (Jira, Trello)	PMBOK, PRINCE2, ISO 21500
Econometric Audit	Quantitative analysis of IT solution cost-effectiveness	Forecasting costs/revenues, investment justification	Statistics, regression (R, Python, Excel)	COBIT, ITIL, ISO/IEC 38500
UX and User Interaction Audit	Usability, accessibility, and interface safety evaluation	Improve user experience, minimize interaction risks	UX testing, WCAG audit, A/B testing	WCAG 2.1, ISO 9241-210, GDPR

*Source: compiled by the authors

Thus, it can be concluded that Digital Audit in the IT industry is a multidimensional process that integrates technical, operational, and ethical aspects to ensure security, efficiency, and compliance with contemporary requirements. The systematization of its core elements in Table 1 underscores the complexity and strategic relevance of this instrument for the sustainable development of IT companies and the maintenance of trust in the digital economy.

This systematization paves the way for understanding the practical significance of Digital Audit, especially in the context of the

specific challenges faced by countries under conditions of instability. In Ukraine, these include military, economic, and integration-related factors that transform auditing from a control mechanism into a key tool for protection, resource optimization, and strategic development of the IT industry.

During wartime, Digital Audit plays a critical role in strengthening the protection of critical infrastructure. Following cyberattacks on state platforms such as Diia, Digital Audit has been instrumental in identifying vulnerabilities and developing mitigation strategies. It also fosters transparency in public and defense-related IT projects, minimizing the risks of overpaying for software, optimizes corporate expenditures by reducing redundant cloud services or improving tax compliance, and, in the context of European integration, ensures alignment with EU standards, such as the NIS2 Directive. The implementation of this directive is a vital step towards Ukraine's integration into the EU Digital Single Market – one of the key milestones on the path to EU accession. Consequently, Digital Audit is no longer a formality but becomes a tool for the survival and development of the IT sector amid war and post-war recovery.

Moreover, Digital Audit has acquired strategic importance for ensuring the transparency, efficiency, and security of Ukraine's IT sector. Its practical application covers several critical areas, among which taxation, public procurement, and post-war reconstruction hold particular significance.

In the field of taxation, Digital Audit contributes to enhanced financial discipline by significantly reducing the share of shadow operations. This is achieved through the implementation of electronic invoicing, automated tax control systems, and the integration of blockchain technologies into state digital platforms to ensure transparency of financial flows. Automated reporting enables the real-time detection of anomalous transactions, minimizes human error, and enhances the accuracy of accounting procedures, particularly in the cloud services segment (SaaS).

In public procurement, Digital Audit functions as a preventive mechanism against corruption risks by analyzing tender documentation on transparent procurement platforms. This improves the efficiency of budget resource allocation and strengthens public trust in the system of public finance.

In the context of post-war recovery, Digital Audit is also an indispensable mechanism for overseeing the effective implementation of reconstruction programs. This includes auditing digital systems used in recovery projects, as well as logistics IT solutions designed for the distribution of international humanitarian and financial aid. The audit process enables the identification of inefficiencies, the minimization of resource losses, and the timely reallocation of funds to areas of critical need.

At the same time, the implementation of Digital Audit in Ukraine is accompanied by a number of significant challenges that require a systematic approach to overcome. One of the most pressing issues is the shortage of qualified personnel and the changing competency profile of auditors. For instance, the Association of Chartered Certified Accountants (ACCA) has already recognized digital literacy as one of the core competencies for professional accountants. However, as early as 2017, the skills of university graduates covered only 45% of the competencies required for the digitally transformed accounting profession [23, p. 207].

Additional barriers include the lack of unified digital audit methodologies, which complicates their adaptation to heterogeneous IT systems, as well as the significant technical and financial costs required for the integration of new technological solutions with existing infrastructures. The escalation of cyber risks under martial law, particularly concerning critical infrastructure, necessitates stricter requirements for the security of audit procedures and data protection.

Financial constraints, driven by the shift in governmental and corporate priorities toward ongoing operational needs, along with organizational resistance to innovation due to limited awareness or bureaucratic inertia,

significantly hinder the pace of Digital Audit development in Ukraine.

To enhance the effectiveness of Digital Audit in the IT industry, it is essential to improve both technological and methodological approaches that account for the dynamic nature of the digital environment. Integrated analytics systems that consolidate data from logs, audit trails, and security metrics offer a holistic view of IT infrastructure and business processes. Platforms supported by Big Data technologies and data visualization tools such as Tableau or Power BI facilitate the processing of complex datasets and the real-time detection of anomalies, which is critical for timely risk mitigation.

The rapid pace of technological advancement necessitates continuous auditor training through certifications, knowledge exchange, and targeted workshops. The creation of internal expert groups focused on specific technologies—such as cloud environments or artificial intelligence systems—can enhance team competencies. Flexible methodological frameworks, which combine traditional standards such as ISO 27001 with risk-based innovative methods, allow for customization to the unique characteristics of each IT system. Investments in advanced technologies, including AI and ML, enable automation of routine tasks, discovery of complex patterns, and risk prediction, such as identifying anomalies in cloud spending or code, thereby deepening the audit process.

In the context of Ukraine's European integration ambitions, Digital Audit gains strategic importance in aligning the IT industry with European standards. The European Union Agency for Cybersecurity (ENISA) emphasizes that candidate countries, including Ukraine, must ensure that their training programs comply with the European Cybersecurity Skills Framework (ECSF) – a practical tool for defining and articulating tasks, competencies, skills, and knowledge for cybersecurity roles in Europe [10].

This necessitates the development of national professional training programs within Ukrainian higher education institutions that enable graduates to obtain internationally recognized certifications such as CISA (Certified Information Systems Auditor), issued by ISACA. These certifications are crucial not only for engineers but also for IT auditors tasked with ensuring compliance with ISO 27001 and GDPR. To support this, it is necessary to develop unified training standards and audit requirements that adapt international norms to the national context, which will facilitate the harmonization of methodologies and integration with European regulatory frameworks.

The implementation of GDPR and accessibility standards such as WCAG 2.1 will also require audits of data processing procedures and digital service functionality. These measures will enhance trust in the Ukrainian IT sector and attract foreign investment. Such efforts not only fulfill European integration obligations but also stimulate the growth of the digital economy, emphasizing the role of auditing in promoting stability and competitiveness.

Digital Audit offers substantial benefits to IT companies by enhancing efficiency and resilience. Automation of procedures reduces audit duration and costs, while AI and Big Data technologies improve analytical accuracy, mitigating the risk of undetected errors or fraud. Integrated systems enable real-time processing of large data volumes, ensuring the relevance of audit findings. The possibility of continuous auditing, supported by persistent system monitoring, improves the quality and timeliness of assessments. These advantages provide IT companies with reliable insights into financial and operational processes, supporting strategic development and strengthening market positions.

However, the implementation of Digital Audit also involves certain limitations. High upfront investments in technologies such as AI or integrated platforms may be burdensome for companies with limited resources. The integration of new tools with legacy systems often presents technical difficulties that require specialized expertise. Auditing large data volumes increases privacy risks, particularly in the context of

wartime cyber threats. The rapid pace of technological change necessitates continuous system upgrades, which can strain corporate resources. Additionally, the lack of historical data makes it difficult to evaluate the long-term effectiveness of new technologies, adding uncertainty to strategic planning.

Conclusion. Digital Audit is a critically important tool in the IT industry, ensuring business stability, security, and efficiency amid ongoing digital transformation. It integrates innovative technologies such as cloud computing, artificial intelligence (AI), machine learning (ML), and blockchain, which enhance the accuracy and quality of audit procedures, enabling IT companies to obtain reliable insights into financial and operational processes. This contributes to the optimization of business workflows, increased competitiveness, and sustainable development in a dynamic digital environment.

However, the implementation of digital audit presents several challenges, including the need for significant investment, data security assurance, the complexity of integrating new technologies, and the rapid pace of technological advancement. Overcoming these barriers requires continuous auditor training, the application of flexible methodologies, a systemic approach, and close cooperation between auditing firms and the IT industry.

The future of digital audit in the IT sector is closely tied to the continued evolution of technologies that enable continuous monitoring, predictive analytics, and automation. These advances will strengthen its role as an indispensable component of risk management and strategic development, supporting compliance with modern standards and enhancing the global competitiveness of companies in the digital economy.

References

1. Al Shanti, N., Mariani, L., & Signori, S. (2024). *The engagement in fraudulent behavior – social aspects. Università degli studi di Bergamo*. 121 p. Available at: https://core.ac.uk/download/630969068.pdf (Accessed 21 March 2025)

2. Alles, M. G. (2015). Drivers of the use and facilitators and obstacles of the evolution of Big Data by the audit profession. *Accounting Horizons, 29*(2), p. 439–449. https://doi.org/10.2308/acch-51067

3. Alpay, M. F., & Usul, H. (2024). From traditional auditing to information technology auditing: A paradigm shift in practices. *European Journal of Digital Economy Research. Vol.5. Issue. 1. pp. 3–9.* Available at: https://core.ac.uk/download/618257238.pdf (Accessed 14 March 2025)

4. Arens, A. A., Elder, R. J., & Beasley, M. S. (2020). *Auditing and assurance services: An integrated approach* (17th ed.). Boston: Pearson. 912 p.

5. Astakhova, M. M. (2007). Vykorystannia komp'iuternykh informatsiinykh system pry provedenni audytu rezerviv i zabezpechen pidpryiemstva [Use of computer information systems in auditing reserves and provisions of an enterprise]. *Naukovi pratsi Kirovohradskoho natsionalnoho tekhnichnoho universytetu. Ekonomichni nauky, (12, Part 1)*, pp. 319–324. (in Ukrainian).

6. Ben Ahmed, D. (2026). The Impact of Artificial Intelligence on Accounting Information and Earnings Management: Bibliometric Analysis // Journal of Risk and Financial Management. Vol. 19, № 1. C. 90. https://doi.org/10.3390/jrfm19010090

7. Deloitte. (2022). *2021 Audit Transparency Report* [Electronic resource]. Deloitte UK. Available at: https://www.deloitte.com/uk/en/about/governance/global-impact-report/annual-report-2021/transparency-report.html (Accessed 21 March 2025)

8. DOU. (2025, April). Skilky aitivtsiv v Ukraini: rekordna kilkist zakrytykh IT-FOPiv za rik [How many IT specialists are in Ukraine: A record number of closed IT sole proprietors in a year]. Available at: https://dou.ua/lenta/articles/how-many-devs-in-ukraine-2025/ (Accessed 25 March 2025) (in Ukrainian).

9. Eamonn O'Raghallaigh. What is a digital audit and why is it important? *Digital Strategy Consultants*. Available at: https://digitalstrategy.ie/insights/what-is-a-digital-audit-and-why-is-it-important/ (Accessed 18 March 2025)

10. ENISA. (2023). *Cybersecurity skills framework for EU candidate countries*. Athens: European Union Agency for Cybersecurity. Available at: https://www.enisa.europa.eu/topics/skills-and-competences/skills-development/european-cybersecurity-skills-framework-ecsf (Accessed 21 March 2025)

11. Kokina, J., Pachamanova, D., & Corbett, A. (2017). The role of data and analytics in the audit profession. *Journal of Emerging Technologies in Accounting, 14*(1), pp. 115–122. https://doi.org/10.2308/jeta-51785 (in Ukrainian).

12. Korol, S. Ya. (2020). Tsyfrovi tekhnolohii v obliku y audyti [Digital technologies in accounting and auditing]. *Derzhava ta rehiony. Seriia: Ekonomika ta pidpryiemnytstvo, 1*, pp. 170–176. Available at: http://nbuv.gov.ua/UJRN/drep_2020_1_31. (Accessed 7 March 2025) (in Ukrainian).

13. Kriukova, I. O. (2022). Rozvytok tsyfrovoho audytu [Development of digital audit]. In *Stratehichni priorytety rozvytku bukhhalterskoho obliku, audytu ta opodatkuvannia v umovakh hlobalizatsii: Materialy mizhnarodnoi naukovo-praktychnoi internet-konferentsii* (pp. 43–45). Sumy: SNAU. (in Ukrainian).

14. Lois, P., Drogalas, G., Karagiorgos, A., & Tsikalakis, K. (2020). Internal audits in the digital era: Opportunities, risks and challenges. *EuroMed Journal of Business, 15*(2), pp. 205–217. https://doi.org/10.1108/EMJB-07-2019-0097

15. Manita, R., Elommal, N., Baudier, P., & Hikkerova, L. (2020). The digital transformation of external audit and its impact on corporate governance. *Technological Forecasting and Social Change, 150*, Article 119751. https://doi.org/10.1016/j.techfore.2019.119751

16. National Bank of Ukraine. *Statystyka zovnishnoho sektoru* [External sector statistics]. Available at: https://bank.gov.ua/ua/statistic/sector-external (Accessed 9 March 2025)

17. Nezhyva, M., & Miniailo, V. (2020). Digitalization of audit in the conditions of the COVID-19. *Herald of Kyiv National University of Trade and Economics, 131*, pp. 123–134. https://doi.org/10.31617/visnik.knute.2020(131)09

18. Pinto, A.R.O. (2024). *A framework for leveraging IT audit using artificial intelligence*. Available at: https://core.ac.uk/download/621578983.pdf

19. Power, M. (1997). *The audit society: Rituals of verification*. Oxford: Oxford University Press. 200 p.

20. PwC. (2021). *Transparency Report 2021* [Electronic resource]. PwC UK. Available at: https://www.pwc.co.uk/who-we-are/transparency-report/2021.html (Accessed 4 April 2025)

21. Tjeng, P. S., & Nopianti, R. (2020). The audit investigation and accounting forensic in detecting fraud in digital environment. *International Journal of Accounting and Taxation, 8*(1), pp. 44–54. https://doi.org/10.15640/ijat.v8n1a6

22. Us, R. L. (2022). Audyt informatsiinykh tekhnolohii yak instrument zabezpechennia efektyvnosti upravlinnia pidpryiemstvom [IT audit as a tool for ensuring effective enterprise management]. *Ekonomichnyi visnyk, 1*, pp. 139–147. (in Ukrainian).

23. Zhyvets, A. N. (2017). Trendy rozvytku profesiinykh kompetentnostei bukhhaltera maloho pidpryiemstva u XXI stolitti [Trends in the development of professional competencies of a small business accountant in the 21st century]. *Aktualni problemy ekonomiky, 6*(192), pp. 204–213. (in Ukrainian).

PECULIARITIES OF DIGITAL AUDIT IN THE IT INDUSTRY: METHODOLOGICAL AND PRACTICAL ASPECTS

Artem Basin, Kyiv National Economic University named after Vadym Hetman, Kyiv (Ukraine).
E-mail: art.basin.itvm@gmail.com
Olena Petryk, Kyiv National Economic University named after Vadym Hetman, Kyiv (Ukraine).
E-mail: auditlena@ukr.net
Yuliia Slobodianyk, Kyiv National Economic University named after Vadym Hetman, Kyiv (Ukraine).
E-mail: yslobodyanik@ukr.net

https://doi.org/10.32342/3041-2137-2026-2-65-10

Keywords: Digital audit, IT industry, cybersecurity, artificial intelligence, blockchain, DevOps, cloud infrastructure, regulatory compliance, data governance, sustainable development
JEL classification: *D83, L86, M15, M45*

This article examines the theoretical and practical aspects of Digital Audit in the IT industry, highlighting the transformation of auditing practices under digitalization. It demonstrates that enhancing audit efficiency through digitalization demands new approaches, tools, methods, and auditor upskilling. Multidimensional taxonomic models of Digital Audit and their specific implementation in IT companies are characterized. The Digital Audit toolkit is defined, considering IT industry functional characteristics, and its development prospects are substantiated through the integration of artificial intelligence and blockchain. Conclusions are drawn and strategic recommendations are proposed for IT industry auditors regarding Digital Audit implementation, considering Ukraine's integration into the European economic space.

The study's relevance stems from digital audit's role in optimizing business processes and ensuring investor confidence. AI integration is crucial for enhancing audit accuracy and timeliness, leading to Digital Audit, highly pertinent to the IT sector.

The implementation of advanced technologies (AI, cloud computing, blockchain, automation) not only accelerates audit but also redefines auditor skill requirements, demanding technological fluency and critical thinking. This introduces risks like data governance and algorithmic bias. The research emphasizes balancing human expertise and technology for effective oversight. Digital Audit in the IT industry is a multidimensional process covering technical, operational, and ethical aspects. Its strategic importance for sustainable IT company development and maintaining digital economy trust is significant. During wartime, digital audit aids in protecting critical infrastructure, identifying vulnerabilities, increasing transparency in government and defense IT projects, and ensuring international standard compliance. It is a vital mechanism for overseeing post-war recovery. Challenges include personnel shortages, lack of unified methodologies, high costs, and cyber risks. Continuous training and investment in advanced technologies are necessary for enhanced effectiveness.

Дата надходження до редакції / Submitted: 03.06.25
Дата прийняття до публікації / Accepted: 29.01.26
Дата публікації / Published: 02.07.2026