https://doi.org/10.53360/2788-7995-2025-4(20)-9

IRSTI: 81.93.29

Z.B. Mukhtarova[*], A.T. Zharkimbekova[1], B.T. Smailova[2]
[1]L.N. Gumilyov Eurasian National University,
010000, Republic of Kazakhstan, Astana, 2 Kanysh Satpayev Street
[2]Shakarim University,
071412, Republic of Kazakhstan, Semey, 20 A Glinka Street
[*]e-mail: zamira_bekenovna@mail.ru

COMPARATIVE ANALYSIS OF AUDIT METHODS FOR INFORMATION SECURITY MANAGEMENT SYSTEMS IN KAZAKHSTAN AND OTHER COUNTRIES

Abstract: *This article presents a comparative analysis of approaches to auditing Information Security Management Systems (ISMS) used in the Republic of Kazakhstan and other countries. The study examines key audit methodologies, including international regulatory frameworks such as ISO/IEC 27001 (International Organization for Standardization / International Electrotechnical Commission), NIST (National Institute of Standards and Technology), and the GDPR (General Data Protection Regulation), with a particular focus on their adaptation across different legal jurisdictions. Special attention is given to the strengths and limitations of various auditing practices, as well as the maturity levels of ISMS executions across different nations. The paper analyzes the current state of information security in Kazakhstan, taking into account the national regulatory landscape and the practical application of audit mechanisms in both public and private sectors. It also identifies critical challenges faced by organizations, such as the shortage of qualified personnel, difficulties in implementing contemporary standards and technologies, and weak interdepartmental coordination. Prospective directions for enhancing ISMS audit methods are outlined based on an evaluation of global best practices. Additionally, the paper discusses potential directions for enhancing ISMS auditing practices by drawing on global experience and offers practical recommendations for improving audit effectiveness and strengthening national cybersecurity frameworks.*

The findings of this study are of practical relevance to information security professionals, auditors, researchers, and organizations involved in risk management and data protection within the context of ongoing digital transformation.

Key words: *audit, information security, information security management systems (ISMS), cybersecurity, legal regulation, international standards, ISO/IEC 27001, risk management.*

Introduction

Worldwide, attention to information security is constantly growing and becoming one of the key aspects of organizational activities. A significant role in this field is played by the audit of ISMS, which ensures compliance with standards and best practices, such as ISO 27001.

According to International Organization for Standardization (ISO) 27001, ISMS is part of an organization's overall management system, based on business risk assessment and ensuring the creation, implementation, operation, monitoring, review, maintenance, and development of information security [1].

An information security management system provides the necessary level of protection for an organization's information system, significantly reducing security threat risks. It functions as a unifying framework that brings together diverse mechanisms and tools for information protection and serves as a core component of a comprehensive organizational security system. Given the sensitivity and value of data processed, stored, and transmitted information systems, any compromise – whether loss, alteration, or unauthorized access – can result in serious financial damages. Therefore, the implementation of an ISMS must be grounded in a rigorous evaluation of its functional alignment with the organization's critical operational requirements [2].

The principal responsibilities of an ISMS may be summarized as follows:

– Detecting external and internal security threats, that may impact business processes of the organizations.

– Evaluating existing information security risks, implementing appropriate risk management measures, and aligning decisions with strategic business objectives.

– Reducing risk levels and actual damages from security incidents.

– Ensuring effective management of ISMS-related processes, including in critical situations.

– Uncovering system weakness and addressing them proactively.

– Clearly defining employee responsibilities in the field of information security.

– Prioritizing the allocation of resources to critical systems and processes that face the highest threat exposure.

– Developing a long-term strategy for ISMS improvement aligned with growth trends of the company.

– Improving the image and trustworthiness of the organization among potential investors and stakeholders in domestic and international arenas.

Information security management system audits are crucial for ensuring data protection and minimizing risks in the context of digital transformation. As we all know, countries worldwide implement specific audit methods based on international standards, regulatory requirements, and corporate practices. According to data provided by Control Case, in October 2022 the International Organization for Standardization published the updated version of ISO/IEC 27001:2022, which will come into effect in October 2025. This version introduces revisions and enhancements aimed at improving the effectiveness of ISMS [3].

Conducting a comparative analysis of traditional ISMS audit methods in Kazakhstan and other countries will help identify the most effective approaches and determine areas for improvement. Such an analysis facilitates the adaptation of global best practices while considering local specifics, thereby enhancing the effectiveness of ISMS audits and ensuring compliance with contemporary information security requirements.

Materials and methods

Conventional approaches to auditing an ISMS of organizations involve a systematic evaluation of digital infrastructures, cybersecurity frameworks, and internal regulatory mechanisms to determine their alignment with recognized standards and best practices in the field of information protection. Its main goal is to analyze the security level of automated systems and identify potential vulnerabilities that could affect their reliability and security. The following key types of audits can be distinguished within this task, according to the classification Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. [4]:

1. Instrumental analysis of the security of automated systems, which includes verification and assessment of the availability and effectiveness of security tools such as antivirus programs, firewalls, intrusion detection systems, and other tools.

2. Analysis of automated systems for compliance with international standards and regulatory requirements. The assessment is carried out based on recommendations of international standards as well as regulatory documents such as ST RK, GOST, and industry standards, indicated at the following link [5].

3. Expert assessment of the security of automated systems. This type of audit involves a detailed examination of the system and its components to identify potential vulnerabilities and analyze the effectiveness of existing security measures.

4. Integrated audit methodology, which represents a thorough examination of the automated system using various methods and tools. This approach ensures the full identification of systemic weakness and potential cybersecurity threats [6,7].

An ISMS audit is conducted to obtain independent and objective data on the current security status of the information infrastructure and to identify existing vulnerabilities. It can be classified into two main categories depending on the methods of its implementation.

Information security audits can also be classified into internal and external audits.

External audit is a one-time procedure initiated by management, shareholders, or an organization. It is conducted by an independent auditor who has no commercial or other vested interests in the audited organization, ensuring objectivity and impartiality of the assessment [8].

External information security audit is a required procedure for governmental and private organizations that own or use confidential information subject to protection. Additionally, it is required for organizations operating key information and telecommunication infrastructure facilities. This type of audit is conducted in accordance with current regulatory acts, standards, and regulations governing information security assessment. It is recommended to conduct external audits regularly to ensure compliance with established requirements and enhance the defense of information assets.

Internal information security audit is organized by the organization itself or on its behalf for internal purposes and may serve as the basis for declaring compliance with standards or regulations for information protection and security. The internal audit is carried out by a specialized structural division of the company or its employees who report directly to the company's management and work within its structure.

This research work employs a relative analysis methodology, adjusting in three key objects:

1. Regulatory frameworks, which mean examination of national laws and international standards governing ISMS audits in Kazakhstan, the United States, the European Union, and Russia.

2. Audit approaches, which mean evaluation of audit techniques, including manual inspections, automated tools, compliance verification, and risk-based assessments.

3. Implementation challenges, which mean identification of barriers to effective ISMS audits in Kazakhstan, such as regulatory gaps, lack of automation, and workforce constraints.

Primary sources include national laws, international security standards, and reports from cybersecurity agencies. Secondary sources consist of academic papers, industry reports, and case studies on ISMS audits.

This study uses a parallel comparison of ISMS audit methods based on specific aspects of information security: Legislative regulation, standards, audit methods, automation, main focus.

In Kazakhstan, traditional ISMS audit methods are also based on these principles; however, local factors such as the maturity level of technology and the presence of legislative norms influence their application.

ISMS audits in Kazakhstan are conducted both as part of internal organizational inspections and through external oversight by government authorities. A significant feature is the regulation of security requirements, which has become increasingly stringent in recent years due to the active development of the digital economy and the growing cyber threat landscape.

Currently, Kazakhstan has several regulatory documents governing information protection and auditing activities in the field of information security. One such document is the Law of the Republic of Kazakhstan «On Personal Data and Their Protection» (2013), as well as regulations concerning requirements for state secret protection and access management [9, 10].

Traditional audit methods used in Kazakhstan include:

- Compliance verification with international security standards, such as ISO/IEC 27001, which is one of the most widely adopted standards for ISMS audits in the country.
- Analysis of security policies for compliance with legal requirements, including data protection regulations such as the Law of the Republic of Kazakhstan «On Personal Data and Their Protection».

Key laws and standards in Kazakhstan:

- Law of the Republic of Kazakhstan «On Informatization» (2015).
- Law of the Republic of Kazakhstan «On personal data and their protection» (2013).
- Law of the Republic of Kazakhstan «On national security of the RK» (2012).
- GOST RK ISO/IEC 27001-2015 – ISMS.
- GOST RK ISO/IEC 27002-2015 – Code of practice for information security management.
- ST RK ISO/IEC 15408 (Common criteria).
- National regulations and orders of the National security committee of the Republic of Kazakhstan (NSC RK) – regulations on the protection of state information systems and critical information infrastructure.

Kazakhstan’s approach to information security combines elements of international standards with local regulatory frameworks. According to research Isabaeva S.B., this strategy allows the country to effectively adapt global cybersecurity practices while considering national specifics [11].

An analysis of the regional distribution of audit firms shows that the highest concentration is in Almaty, with 208 companies (43.2% of the total). Other key centres include Astana (137 organizations, or 28.5%) and Shymkent (27 organizations, or 5.6%).

According to the Ministry of Finance of the Republic of Kazakhstan, the total number of auditors in the country exceeds 1.6 thousand. Over the past five years, there has been a significant increase in their numbers. In 2022–2023 alone, 1.3 thousand new specialists entered the field, surpassing the total growth of auditors over the previous 25 years of the profession's existence in Kazakhstan [12].

Results and discussion

In Kazakhstan, auditing is conducted both manually and using automated systems. However, compared to developed countries, such systems are still insufficient, making deeper and more efficient inspections more challenging.

In countries with developed economies, the approach to ISMS auditing is more formalized, with extensive use of automated systems and security standards.

In the United States, traditional ISMS audit methods adhere to strict standards and requirements regulating all aspects of information security. One of the primary standards used for auditing is NIST 800-53, which provides detailed security requirements for information systems [13]. The United States audit system accent risk analysis, including quantitative assessment methods for vulnerabilities and threats. An essential element is the integration of auditing with security policies and incident management processes.

In the European Union, ISMS auditing is regulated by the General Data Protection Regulation, which sets strict requirements for the processing of personal data. To ensure compliance with the GDPR, organizations conduct regular checks and audits, including an assessment of the security of IT systems and an audit of the access control mechanism [14]. Auditing in the EU is usually carried out using automated tools, such as SIEM systems, which allow for real-time monitoring of the security status and detailed reporting on risks and vulnerabilities.

In Russia, traditional ISMS audit methods are regulated by number of federal laws, such as the Federal Law on Information Protection and Federal Law No. 152 «On personal data». The GOST R 56939-2016 standard, which is an analogue of ISO/IEC 27001, is also used.

As in Kazakhstan, traditional audit methods, such as internal documentation review and risk analysis, are actively used in Russia, but the implementation of automated systems is currently limited. Comparative analysis of ISMS audit processes in Kazakhstan and other countries is shown in the Table 1.

Table 1 – Comparative analysis of the processes of conducting an ISMS audit

Criterion	Kazakhstan	USA	EU	Russia
Legislative Regulation	Law of the Republic of Kazakhstan «On personal data protection», government regulations, ST RK 34.015-2018	NIST 800-53, FISMA, HIPAA, CISA, ISO/IEC 27001	GDPR, national standards (e.g., Cyber Essentials), NIS2 Directive	Federal laws (FZ-152, FZ-187, FZ-149), GOST R 56939-2016, FSTEC Order No. 17
Standards Used	ISO/IEC 27001, ST RK 27001, 27002, 15408, 27005	ISO/IEC 27001, NIST SP 800-53, NIST Cybersecurity Framework, PCI DSS, SOC 2	ISO/IEC 27001, Cyber Essentials, GDPR, ENISA guidelines	GOST R 56939-2016, ISO/IEC 27001, STR-K, FSTEC and FSB methodologies
Audit Methods	Manual and automated, compliance checks	Integration of audit with security policies, risk analysis	Compliance checks with GDPR, automated incident monitoring	Risk analysis, physical security assessment, compliance with FSTEC requirements
Automation	Limited, initial-stage use of automated tools (SIEM, DLP, IDS/IPS, MaxPatrol, Nessus, sandboxing, IDIAR systems)	Widely used: SIEM (Splunk, IBM QRadar, Microsoft Sentinel), SOAR, AI/ML, cloud solutions	Comprehensive audit platforms, including GRC (SAP GRC, OneTrust)	Vulnerability analysis systems (MaxPatrol, Security Vision, Positive Technologies), compliance management platforms (Code Security, AKAD)
Main Focus	Compliance with legislation, physical security	Integration of security into risk management processes	Personal data protection, audit process automation	Personal data protection, compliance with legislation

Global practice highlights the critical importance of information security at both the state and private sector levels. However, in Kazakhstan, based on the information above, the primary focus is on protecting government institutions, while information security issues in commercial organizations remain underdeveloped.

Kazakhstan's regulatory framework is evolving but remains largely compliance-driven rather than risk-oriented. While ISO/IEC 27001 provides a foundation, enforcement mechanisms and automation lag behind those in the US and EU.

Also, Kazakhstan faces several challenges in the implementation of effective ISMS audits, limiting their efficiency and overall impact on cybersecurity. Key issues include reliance on manual processes, a shortage of skilled auditors, regulatory inconsistencies, and low adoption rates in the private sector.

This difference in priorities highlights the need for a comprehensive approach to cybersecurity that encompasses not only the public but also the commercial sector. In this regard, two prominent research institutions play a critical role by providing comprehensive evaluations of global cybersecurity readiness. Their research helps to identify vulnerabilities in information protection and contributes to raising awareness of key aspects of information security, which can form the basis for developing a more balanced and effective cyber defense strategies, particularly relevant for Kazakhstan.

1. The Global Cybersecurity Index (GCI) is a joint project of the International Telecommunication Union (ITU) and ABI Research aimed at assessing the capabilities of states in the field of cybersecurity, according to the information [15]. It reflects the extent to which countries prioritize cybersecurity on the international stage and promotes awareness of the essential components required for safeguarding digital infrastructure [16].

2. The National Cyber Security Index (NCSI) is a global indicator that assesses the readiness of states to prevent cyber threats and cybercrime. Additionally, to the rating function, NCSI is an open database with evidence, analytical materials and tools aimed at developing national potential in the field of cybersecurity. This index is developed and maintained by the academy of Electronic Governance Foundation [17].

Kazakhstan is actively working to improve its positions in these ratings by developing state information security programs and implementing measures to protect critical infrastructure, developing cyber threat monitoring centers and strengthening control over digital risks. However, in order to further improve rating positions, it is necessary to continue working on strengthening the regulatory framework, improving technical solutions and raising public awareness in the field of digital security.

According to the research of S.B. Isabaeva, to ensure cybersecurity in Kazakhstan, it is necessary to form an effective legislative system. Considering international experience (Singapore, USA, Great Britain, China) and the requirements of the GDPR, it is advisable to develop a national law on cybersecurity, implement a «cyber insurance» system and clearly define this term in the NPA of the Republic of Kazakhstan. Additionally, enhancing cybersecurity governance will require active engagement from the private sector to foster more efficient protection mechanisms. The low level of cybersecurity in Kazakhstan implies a high possibility of vulnerability to hacker attacks, as well as cybercrimes. Moreover, Kazakhstan's practice shows the need to improve regulatory activities due to frequently introduced amendments and additions to legislation, including the Laws of the Republic of Kazakhstan «On informatization», «On national security», «On personal data and their protection» [18, 19].

The comparison of ISMS audit practices in Kazakhstan and other countries illustrates notable differences and similarities. While Kazakhstan is making strides in aligning with international cybersecurity standards, its approach remains largely compliance-driven, particularly focusing on government institutions. The US and EU, in contrast, have a more risk-oriented and automated auditing approach, with extensive use of advanced tools like SIEM, SOAR, and AI/ML to ensure real-time monitoring and compliance. This enables more proactive threat detection and continuous monitoring.

Furthermore, the low level of private sector involvement in cybersecurity audits in Kazakhstan highlights a key gap in the overall strategy. The private sector remains underdeveloped in terms of cybersecurity measures compared to the public sector. For Kazakhstan to improve its cybersecurity posture, it is essential to foster greater collaboration between government and private entities,

strengthen enforcement mechanisms, and develop a more comprehensive risk-based approach to ISMS audits. Adapting proven international practices and investing in technological innovation are key to narrowing the gap and increasing audit effectiveness. Conducting a more in-depth assessment of audit automation maturity across different sectors could help identify specific technological and organizational challenges that hinder further advancement.

However, the successful implementation of these activities may be constrained by several factors, such as limited financial investment, underdeveloped research infrastructure, and shortage of qualified experts in cybersecurity and artificial intelligence. Enhancing cooperation between universities, industry stakeholders, and government bodies is therefore crucial to address these challenges and to ensure that the automation of ISMS audits in Kazakhstan achieves practical and sustainable outcomes.

Conclusion

In conclusion, the cross-country comparison of ISMS audit practices reveals substantial differences in both methodological sophistication and system maturity. While Kazakhstan actively employs the ISO/IEC 27001 standard, its audit processes are still in an early phase when contrasted with the more integrated and technological advanced systems found in the US and EU.

Kazakhstan faces several challenges, including defined automation of audit processes, insufficient technical infrastructure, and limited capabilities for real-time threat analysis. However, the country has all the necessary foundations for further development. A key step for Kazakhstan will be the development of human resources, increasing technological maturity, and expanding the use of automated risk monitoring and analysis systems. Implementing a comprehensive approach, as seen in the US and EU, could be an ideal model for Kazakhstan, enabling not only improved audit efficiency and accuracy but also strengthening the overall information security framework.

Therefore, improving audit methodologies remains a critical objective for Kazakhstan, one that will require sustained effort, targeted investment, and institutional regulation. However, the proposed hybrid model, which merges international expertise with local contextual needs, presents a promising framework for building resilient and globally competitive information security system.

References

1. ISO/IEC 27001. Information technology – Security techniques – Information security management systems – Requirements (TechNormative Ed.), 2006.
2. Averchenkov B.I. Audit informacionnoj bezopasnosti: metodologija i praktika. – Moskva: Nauka, 2021. (In Russian).
3. Important changes to ISO 27001:2022: https://www.controlcase.com/important-changes-to-iso-27001/?utm_source=chatgpt.com (accessed: 14.03.2025).
4. The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda / G. Culot et al // The TQM Journal, 2021.
5. ST RK ISO/IEC 27001-2015 «Informacionnaja tehnologija. Metody i sredstva obespechenija bezopasnosti. Sistemy menedzhmenta informacionnoj bezopasnost'ju. Trebovanija». – 2015. (In Russian).
6. De la Rosa Martín T. Automation of an information security management system based on the ISO/IEC 27001 Standard // Revista Universidad y Sociedad. – 2021. – Vol. 13, № 5. – P. 495-506.
7. Al-Karaki J.N. GoSafe: On the practical characterization of the overall security posture of an organization information system using smart auditing and ranking / J.N. Al-Karaki, A. Gawanmeh, S. El-Yassami // Journal of King Saud University – Computer and Information Sciences. – 2022. – Vol. 34, № 6. – P. 3079-3095.
8. Bakpokpaev A.A. Klassifikacija i analiz metodov i sredstv audita informacionnoj bezopasnosti / A.A. Bakpokpaev, E.Zh. Ajthozhaeva. – Almaty: Universitet im. Satpaeva, 2022. (In Russian).
9. Zakon Respubliki Kazahstan «O personal'nyh dannyh i ih zashhite». – 2013. (In Russian).
10. Zakon Respubliki Kazahstan «O bezopasnosti». – 2005. (In Russian).
11. Isabaeva S.B. Obespechenie kiberbezopasnosti Kazahstana v uslovijah global'noj cifrovizacii: Doktorskaja dissertacija. – Kazahstan, 2020. (In Russian).
12. Berezjuk V.I. Perspektivy razvitija cifrovogo audita v Respublike Kazahstan v uslovijah perehoda k cifrovoj jekonomike // Uchet. Analiz. Audit. – 2024. – T. 11(1). – S. 27-38. (In Russian).
13. National Institute of Standards and Technology (NIST). Security and privacy controls for federal information systems and organizations. – 2018.
14. European Union. General Data Protection Regulation (GDPR). – 2016.

15. International Telecommunication Union, ABI Research. Global cybersecurity index & cyberwellness profiles. – Geneva: ITU, 2015. – Available at: http://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf (accessed: 14.03.2025).
16. International Telecommunication Union. The Global Cybersecurity Index. – 2020. – Available at: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx (accessed: 14.03.2025).
17. E-Governance Academy. The National Cyber Security Index. – 2020. – Available at: https://ncsi.ega.ee/methodology/ (accessed: 14.03.2025).
18. Kompanijalardyң aқparattyқ bejimdeu monitoringi / V.A. Lahno et al // QazKKA Habarshysy. – 2023. – T. 6(129). – S. 173-185. (In Kazakh).
19. Automation of information security risk assessment / B. Akhmetov et al // International Journal of Electronics and Telecommunications. – 2022. – Vol. 68, № 3. – P. 549-555. https://doi.org/10.24425/ijet.2022.141273.

З.Б. Мухтарова[*], А.Т. Жаркимбекова[1], Б.Т. Смаилова[2]
[1]Л.Н. Гумилев атындағы Еуразия ұлттық университеті,
010000, Қазақстан Республикасы, Астана қ., Қаныш Сәтбаев к-сі, 2
[2]Шәкәрім университеті,
071412, Қазақстан Республикасы, Семей қ., Глинки к-сі, 20 А
[*]e-mail: zamira_bekenovna@mail.ru

АҚПАРАТТЫҚ ҚАУІПСІЗДІКТІ БАСҚАРУ ЖҮЙЕЛЕРІН АУДИТТЕУ ӘДІСТЕРІНІҢ ҚАЗАҚСТАНДАҒЫ ЖӘНЕ БАСҚА ЕЛДЕРДЕГІ САЛЫСТЫРМАЛЫ ТАЛДАУЫ

Мақалада Қазақстандағы және басқа елдердегі ақпараттық қауіпсіздікті басқару жүйелерінің (АҚБЖ) аудитінің дәстүрлі әдістерінің салыстырмалы талдауы берілген. Мақалада аудит процесінде қолданылатын негізгі тәсілдер, соның ішінде ISO/IEC 27001 (Халықаралық стандарттау ұйымы/Халықаралық электротехникалық комиссия), NIST (Ұлттық стандарттар және технологиялар институты), GDPR (деректерді қорғаудың жалпы ережесі) және олардың әртүрлі юрисдикцияларда бейімделуі сияқты халықаралық стандарттар талқыланады. Әр әдістің артықшылықтары мен кемшіліктеріне, сондай-ақ әртүрлі елдердегі ақпараттық қауіпсіздікті басқару жүйелерінің жетілу дәрежесіне ерекше назар аударылады. Қазақстандағы ақпараттық қауіпсіздіктің ағымдағы жағдайы, оның ішінде нормативтік-құқықтық база және мемлекеттік және жеке ұйымдарда аудит тетіктерін іс жүзінде қолдану талданады. Мамандардың біліктілігінің жеткіліксіздігі, заманауи технологиялар мен стандарттарды енгізу проблемалары, сондай-ақ ведомствоаралық үйлестірудің жоқтығы сияқты ұйымдардың киберқауіпсіздікті қамтамасыз етуде кездесетін негізгі проблемалары мен қиындықтары атап өтілді. Мақалада әлемдік тәжірибені ескере отырып, АҚБЖ аудит әдістерін жетілдіру перспективалары қарастырылып, аудиттің тиімділігін арттыру және ақпараттық қауіпсіздік саласындағы ұлттық тәжірибені жетілдіру жолдары ұсынылады.

Зерттеу нәтижелері ақпараттық қауіпсіздік мамандары, аудиторлар, зерттеушілер, сондай-ақ қазіргі заманғы цифрлық трансформация жағдайында тәуекелдерді басқару және деректерді қорғаумен айналысатын ұйымдар үшін пайдалы болуы мүмкін.

Түйін сөздер: *аудит, ақпараттық қауіпсіздік, ақпараттық қауіпсіздікті басқару жүйелері (АҚБЖ), киберқауіпсіздік, құқықтық реттеу, халықаралық стандарттар, ISO/IEC 27001, тәуекелдерді басқару.*

З.Б. Мухтарова[*], А.Т. Жаркимбекова[1], Б.Т. Смаилова[2]
[1]Евразийский национальный университет им. Л.Н. Гумилева,
Республика Казахстан, г. Астана, ул. Каныш Сатпаева, 2
[2]Шәкәрім университет,
071412, Республика Казахстан, г. Семей, ул. Глинки, 20 А
[*]e-mail: zamira_bekenovna@mail.ru

СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕТОДОВ АУДИТА СИСТЕМ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ В КАЗАХСТАНЕ И ДРУГИХ СТРАНАХ

В статье представлен сравнительный анализ традиционных методов аудита систем управления информационной безопасностью (СУИБ) в Казахстане и других странах. В статье рассматриваются ключевые подходы, используемые в процессе аудита, включая такие

международные стандарты, как ISO/IEC 27001 (Международная организация по стандартизации/Международная электротехническая комиссия), NIST (Национальный институт стандартов и технологий), GDPR (Общий регламент по защите данных), и их адаптация в различных юрисдикциях. Особое внимание уделено преимуществам и недостаткам каждого метода, а также степени зрелости систем управления информационной безопасностью в разных странах. Проанализировано современное состояние информационной безопасности в Казахстане, включая нормативную базу и практическое применение механизмов аудита в государственных и частных организациях. Выделены основные проблемы и вызовы, с которыми сталкиваются организации при обеспечении кибербезопасности, такие как недостаточная квалификация специалистов, проблемы с внедрением современных технологий и стандартов, а также отсутствие межведомственной координации. Также рассматриваются перспективы совершенствования методов аудита СУИБ с учетом мирового опыта и предлагаются пути повышения эффективности аудита и совершенствования национальных практик в области информационной безопасности.

Результаты исследования могут быть полезны специалистам по информационной безопасности, аудиторам, исследователям, а также организациям, занимающимся управлением рисками и защитой данных в условиях современной цифровой трансформации.

Ключевые слова: *аудит, информационная безопасность, системы управления информационной безопасностью (СУИБ), кибербезопасность. правовое регулирование, международные стандарты, ISO/IEC 27001, управление рисками*.

Information about the authors

Zamira Bekenovna Mukhtarova* – 2nd-year doctoral student of the educational program «Information security systems»; L.N. Gumilyov Eurasian National University, Astana, Republic of Kazakhstan; e-mail: zamira_bekenovna@mail.ru. ORCID: https://orcid.org/0009-0003-9072-8475.

Aizhan Temirzhanovna Zharkimbekova – PhD, Senior Lecturer, Department of information security; L.N. Gumilyov Eurasian National University, Astana, Republic of Kazakhstan; e-mail: zh.aizhan.t@gmail.com. ORCID: https://orcid.org/0000-0001-7053-2844.

Balzhan Temirbolatkyzy Smailova – MS, Head of Mathematics Department, NCJSC «Shakarim University»; Semey, Republic of Kazakhstan; e-mail: st.balzhan @gmail.com. https://orcid.org/0009-0005-4932-1774.

Авторлар туралы мәліметтер

Замира Бекеновна Мухтарова* – 2-курс докторанты, «Ақпараттық қауіпсіздік жүйелері» білім беру бағдарламасы; Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана қ., Қазақстан Республикасы; e-mail: zamira_bekenovna@mail.ru. ORCID: https://orcid.org/0009-0003-9072-8475.

Айжан Темиржановна Жаркимбекова – PhD, аға лектор, Ақпараттық қауіпсіздік кафедрасы; Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана қ., Қазақстан Республикасы; e-mail: zh.aizhan.t@gmail.com. ORCID: https://orcid.org/0000-0001-7053-2844.

Балжан Темірболатқызы Смаилова – магистр, математика кафедрасының меңгерушісі, «Шәкәрім Университет» КеАҚ; Семей, Қазақстан Республикасы; e-mail: st.balzhan @gmail.com. ORCID: https://orcid.org/0009-0005-4932-1774.

Сведения об авторах

Замира Бекеновна Мухтарова* – докторант 2-го курса ОП «Системы информационной безопасности»; Евразийский национальный университет им. Л.Н.Гумилева города Астана, Республика Казахстан; e-mail: zamira_bekenovna@mail.ru. ORCID: https://orcid.org/0009-0003-9072-8475.

Айжан Темиржановна Жаркимбекова – PhD, Сеньор-лектор, Департамент информационной безопасности; Евразийский национальный университет им. Л.Н. Гумилева города Астана, Республика Казахстан; e-mail: zh.aizhan.t@gmail.com. ORCID: https://orcid.org/0000-0001-7053-2844.

Балжан Темірболатқызы Смаилова – магистр, заведущая кафедры математики, НАО «Шәкәрім Университет»; Семей, Республика Казакстан; e-mail: st.balzhan@gmail.com. ORCID: https://orcid.org/0009-0005-4932-1774.

Received 16.09.2025
Revised 22.10.2025
Accepted 23.10.2025