Library Science. Record Studies. Informology.

Library Science. Record Studies. Informology. 20(4), 2024, 43-55
Journal homepage: https://bdi.com.ua/en/journals/journal
Received 22.07.2024 Revised 22.10.2024 Accepted 25.11.2024

UDC 006.32 DOI: 10.63009/lsrsi/4.2024.43

The issue of electronic document preservation in the context of international information security standards

Liudmyla Filipova*
Doctor of Pedagogical Sciences, Professor
Kharkiv State Academy of Culture
61057, 4 Bursatsky Dsc., Kharkiv, Ukraine
https://orcid.org/0000-0003-0273-7922

Anna Shelestova
PhD in Science in Social Communications, Acossiate Professor
Kharkiv State Academy of Culture
61057, 4 Bursatsky Dsc., Kharkiv, Ukraine
https://orcid.org/0000-0003-4866-1767

Abstract. The relevance of this study is driven by the rapid development of electronic document management and the growing need for reliable digital data preservation amid contemporary cyber threats and technological challenges. The research aimed to conduct a comprehensive analysis of electronic document preservation issues and develop recommendations for implementing effective electronic records management systems in accordance with international standards. The study employed an analytical method to examine international information security standards, a systems approach to conceptualise document preservation processes as an integrated system, a comparative method to analyse different approaches to electronic document preservation, and a case study method to evaluate practical implementations of electronic document management systems. The findings underscored the critical importance of addressing technological obsolescence of data formats, the complexities of electronic document management processes, and data loss risks. Key aspects of managing and preserving electronic records in line with international information security standards were examined. Emphasis was placed on the necessity of implementing comprehensive strategies to ensure the long-term preservation of digital documents. Six core strategic approaches were identified: adherence to international standards; development of holistic policies for document collection, storage, and access; creation of an operational model for digital preservation; implementation of effective data administration and transfer policies; regular system audits and updates; and provision of adequate staff training and education. Attention was given to the potential of emerging technologies such as blockchain and artificial intelligence, which can enhance the efficiency of electronic document preservation. Blockchain ensured integrity, authenticity, and transparency through decentralised record-keeping, while artificial intelligence technologies optimised document classification, indexing, and retrieval, addressing confidentiality concerns. The need to integrate these technologies in compliance with established international standards to guarantee the authenticity, immutability, and persistent accessibility of electronic documents was highlighted. The practical value of this research lies in its recommendations for implementing a set of best practices for electronic document preservation, including regular material assessments, metadata management, and technological infrastructure maintenance. The study's findings can be utilised by organisations to improve their electronic document management systems and enhance information security levels

Keywords: electronic document management; ISO standards; cybersecurity; digital preservation; metadata management; technological infrastructure

Suggested Citation:
Filipova, L., & Shelestova, A. (2024). The issue of electronic document preservation in the context of international information security standards. *Library Science. Record Studies. Informology,* 20(4), 43-55. doi: 10.63009/lsrsi/4.2024.43.

*Corresponding author

Introduction

In the context of rapid digitalisation spanning 1995-2024, the preservation and protection of electronic documents have been accorded significant importance. At the state level in Ukraine, electronic document management systems have been widely implemented, large-scale digitisation of paper-based and other media documents has been undertaken, and specialised information-communication systems have been established to meet the needs of the country's population.

Under these conditions, the theoretical, methodological, and organisational principles of forming electronic resources, as outlined in the UNESCO Charter on the Preservation of Digital Heritage (2003), have gained particular significance. The Charter defined digital heritage as "a unique repository of human knowledge encompassing cultural heritage originally created in digital form". However, Ukrainian society still insufficiently addressed issues related to the risks of losing photo documents, audio and video recordings, personal or professional correspondence, contacts, files, and other important digitally stored records. These matters played a crucial role in sustainable national development, as state and commercial data were increasingly generated exclusively in digital form, as noted by M. Senchenko (2022).

P. Joseph *et al.* (2012) examined shifts in the documentation management paradigm and their impact on the implementation of the international standard ISO 15489. The authors explored how technological evolution and organisational restructuring alter responsibility distribution for record preservation. The study highlighted challenges associated with the practical application of ISO 15489 and proposed approaches to overcoming institutional barriers. Special attention was devoted to integrating document management systems with other organisational information systems and ensuring compliance with regulatory requirements in document processing.

Challenges in digital preservation included file format management, metadata accuracy assurance, and addressing complexities associated with compound documents. A. Bullock's (1999) research laid the foundational understanding of long-term digital information preservation issues. The author analysed key challenges organisations face, when attempting to ensure the longevity of electronic records, focusing on technological obsolescence, media degradation, and the necessity of maintaining continuous data accessibility.

S. Marulin (2013) proposed developments in information technologies to facilitate efficient data exchange between electronic document management systems and information system databases. The author examined technical aspects of integrating diverse information components and proposed a methodology to optimise data transfer processes. The work addressed issues of format compatibility, data integrity, and information security in inter-system document exchange.

Specific aspects of preserving digital evidence were explored by B. Guttman *et al.* (2022). The researchers provided detailed recommendations for professionals handling electronic documents in legal contexts. The study described methods ensuring the integrity, authenticity, and accessibility of digital evidence throughout its lifecycle, covering critical aspects such as chain of custody, data integrity verification techniques, and strategies for guaranteeing long-term access to digital materials. Compliance with international standards and regulatory requirements was emphasised.

Methods such as technology preservation, emulation, encapsulation, and migration to standardised formats (e.g., XML, ASCII, and PDF/A) were essential for overcoming these challenges and ensuring the prolonged accessibility of digital data. Such a multifaceted approach has become indispensable for maintaining digital documents in a usable form over extended periods, given that the lifecycle of a document's technical format was typically limited to 5-10 years (Information security, n.d.).

Beyond technical aspects of electronic document preservation, semantic protection methods have gained equal importance. Researchers B. Durniak & V. Sabat (2010) examined innovative dimensions of information security in document management systems, focusing on semantic protection methods. The authors analysed issues of ensuring confidentiality, integrity, and availability at the level of document content, presenting theoretical foundations and practical techniques for implementing semantic safeguards to detect unauthorised content alterations and prevent document forgery.

Methodological frameworks for securing electronic document management in hierarchical automated control systems were explored by V. Sabat (2023). The scholar developed theoretical and methodological foundations for information technologies protecting document workflows in hierarchical automated management systems overseeing complex technological processes under active threats and attacks. This has become particularly relevant in the modern era of digital transformation and escalating cyber threats targeting electronic documents and data.

The authors A.L. Cushing & G. Osti (2023) examined the impact of artificial intelligence (AI) technologies on expertise in the field of digital archiving. The scholars also analysed how AI concepts were transforming traditional approaches to digital information preservation, and what new challenges and opportunities it create for archival professionals. The study proposed a conceptual framework for understanding the interaction between human experts and AI systems in the context of digital information preservation. Particular attention

was paid to balancing diverse needs: processing efficiency for large volumes of data, maintaining document authenticity, ensuring accessibility, and protecting confidential information.

The publication by Z. Teel (2024) constituted a significant contribution to research on the application of artificial intelligence technologies for preserving historical archives. The author explored innovative approaches to the digital conservation of cultural heritage using advanced AI algorithms. The study analysed key advantages of AI in archival preservation, including: automation of digitisation and indexing processes for large volumes of historical documents; enhanced accuracy in text and metadata recognition for ancient manuscripts and damaged documents; prediction of digital object degradation and proactive planning of conservation measures; identification of connections and patterns between archival materials, facilitating a deeper understanding of historical context. Special attention was devoted to ethical issues arising from AI applications in archival practice, particularly concerns regarding confidentiality, accurate attribution, and the representativeness of preserved materials. The researcher proposed approaches to ensuring that AI-driven preservation processes comply with international standards and ethical norms. This study was particularly valuable in developing a comprehensive understanding of the role of modern technologies in ensuring the long-term preservation of digital heritage. It complemented the work of A.L. Cushing & G. Osti (2023), which offered a more specialised perspective on the technological aspects of digital preservation of historical documents using artificial intelligence.

The study aimed to examine and systematise methodological approaches to ensuring the long-term preservation of electronic records in accordance with international information security standards.

Materials and Methods

The research employed a comprehensive methodology combining various methods and approaches for a thorough investigation of electronic records preservation within the context of international information security standards. The foundation of the study was the analytical method, which facilitated the examination of international information security standards, particularly ISO 15489-1:2016 (2016) and ISO/IEC 27001:2022 (2022). A systems approach ensured that electronic records preservation processes were considered as an integrated system, where technical, organisational, and regulatory aspects interact and influence one another. The comparative method was used to juxtapose different standards and approaches to electronic records preservation. The case-study method enriched the research with practical examples, including an analysis of the Welsh Journals Project and an examination of the British Library's strategy. An interdisciplinary approach encompassed technical, managerial, and legal dimensions of the research topic. A holistic approach provided a comprehensive examination of the issues, including technological solutions and organisational processes. The predictive approach helped outline future developments in electronic records preservation technologies.

The research strategy was based on documentary analysis of international standards and scholarly publications, examination of practical implementations of electronic records preservation systems, and systematisation of best practices in this field. Given that electronic documentation has become a critical component of business processes across organisations, the need for robust standards to manage these records effectively has emerged. The ISO 15489-1:2016 (2016) standard emphasised the importance of records in business operations and aimed to support electronic records management systems. Furthermore, usability criteria, adaptability across devices, and access control implementation were crucial for maintaining the confidentiality and integrity of sensitive information, as outlined in ISO 14641:2018 (2018). An analysis of ISO 15489-1:2016 (2016) confirmed its fundamental role in shaping modern electronic records management systems. This document, along with the related ISO 14641:2018 (2018), delineated key specifications and organisational policies for the collection, storage, and access to electronic records. This ensured not only access control and record integrity, but also traceability throughout the entire preservation lifecycle. Supporting evidence can be found on the Digital Preservation Coalition (2024) platform, which described the significance of international standards for effective electronic records preservation by organisations.

The ISO/IEC 27000 series, referenced in Publicly Available Standards (2024), constituted information security standards jointly published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). The Complete List of Cyber Security Standards (n.d.) noted that these standards provided a framework of guidelines to support infrastructure – primarily corporate data centres – in adhering to legal, technical, and physical policies to ensure the confidentiality, integrity, and availability of data stored within them. These standards applied to various forms of electronic records, whether created through scanning, conversion from analogue formats, or generated directly within information systems and electronic records management systems. Additionally, the study examined issues of long-term electronic records preservation and data loss risk management (McLeod, 2008). A key source was an analytical report on the Welsh Journals Project, which highlighted practical aspects of document digitisation (Digital Preservation Case Notes…, 2010).

Institutional strategic documents demonstrated the practical implementation of electronic records

preservation principles. A notable example was the British Library Digital Preservation Strategy (2016), which outlined systematic approaches to digital preservation and identified essential components for long-term storage. Institutional digital preservation strategies and policies were examined in sources such as Digital Preservation Strategy 2022-2026 (2022) and Institutional policies and strategies (n.d.), which provided recommendations for developing and implementing relevant policies. Technological aspects of electronic records preservation and obsolescence challenges were addressed in Preservation issues (n.d.), which analysed various strategies for mitigating technological obsolescence and ensuring long-term access to electronic records.

The research's source base encompassed a wide range of materials, from international information security standards to thematic studies and organisational best practices. This comprehensive approach to source selection provided a robust foundation for developing practical recommendations. The chosen methodology not only facilitated an in-depth analysis of electronic records preservation challenges, but also enabled the formulation of specific proposals for improving existing practices in this field.

Results and Discussion

Electronic records preservation faces numerous challenges that organisations must address to ensure long-term accessibility and integrity of digital content. These challenges can be broadly categorised as issues related to format, storage, and the inherent nature of digital objects. One of the primary challenges in electronic records preservation is the rapid obsolescence of file formats and storage media. Access to digital records is only possible through specific combinations of hardware and software, which may become obsolete within a cycle of no more than three years (ISO 19005-4:2020, 2020). Consequently, organisations must continually migrate digital objects to current formats and media to prevent data loss and ensure uninterrupted access (Guttman *et al.*, 2022). The migration process itself can be complex and costly, often requiring specialised expertise for effective management (McLeod, 2008).

The complexity of electronic processes and their interactions also creates challenges for preservation. Organisations employing intricate systems with numerous interdependencies may require extensive documentation to maintain clarity and control over their processes (Biswas, 2023). Over time, such complexity can lead to difficulties in ensuring the preservation of all components of a digital document in a usable form. Furthermore, during document conversion or migration between formats, there is a risk of losing critically important elements of presentation, functionality, and contextual relationships within the data (ISO 19005-4:2020, 2020).

Data loss poses a significant risk in the field of electronic document preservation. Such loss may occur due to hardware failures, viral, spyware, or unlicensed software, cyberattacks, or human error, potentially leading to severe consequences for organisations, including financial losses, legal complications, and reputational damage. A notable example is the large-scale cyberattack in 2023 on Kyivstar, one of Ukraine's largest mobile operators, with all its negative repercussions. Research by J. McLeod (2008) revealed that 93% of companies that lost their data centres for ten or more days filed for bankruptcy within a year of the disaster, underscoring the urgent need for robust backup, redundancy, and data recovery strategies, as well as enhanced organisational cybersecurity measures and employee cyber hygiene.

Organisations must also navigate a diverse array of legislative and regulatory requirements governing electronic document preservation. Different industries and jurisdictions may impose specific standards regarding documentation practices, necessitating careful consideration during the preservation process. Compliance with these requirements adds another layer of complexity, as organisations must ensure adherence to legal and regulatory frameworks while effectively managing their data preservation efforts. Engaging relevant stakeholders in the data preservation process was crucial yet challenging. Input from various departments and external parties was essential for creating and accurately updating documentation (Biswas, 2023).

However, coordinating such stakeholder involvement can be difficult, particularly in large organisations where multiple stakeholders may have divergent priorities or perspectives. Key issues concerning data/information/document preservation are addressed in international information security standards. These play a pivotal role in establishing guidelines and boundaries that organisations can apply to safeguard their electronic resources/information assets. These standards encapsulate best practices for security risk management, ensuring data confidentiality, integrity, and availability across various sectors.

A. Guz (2013) traced the historical development of global information security standards and analysed their transformation under the influence of technological changes. The work examined key standards in information protection, their interrelationships, and practical applications. Particular attention was devoted to the ISO/IEC 27000 series, which regulated the establishment of information security management systems. This study became an important resource for understanding the evolution of approaches to information security in the modern world.

According to E. Zierau *et al.* (2021), ISO/IEC 27001:2022 was the most widely recognised international standard for Information Security Management Systems (ISMS). It outlined requirements for establishing, implementing, maintaining, and continually

improving an ISMS, emphasising a structured approach to managing an organisation's confidential information through risk management processes. The standard defined three key aspects of information security: confidentiality, integrity, and availability, ensuring that information was accessible only to authorised individuals, remained accurate and unaltered, and was available when needed. Organisations implementing ISO/IEC 27001:2022 (2022) may obtain certification, demonstrating their commitment to secure and effective information management. The Center for Internet Security (CIS) has published widely accepted security benchmarks, serving as configuration guides for various IT systems, including mobile devices, network appliances, and web browsers. These benchmarks have been instrumental for organisations seeking to assess and enhance the security of their IT infrastructure (Teel, 2024).

D. Antonucci (2017) presented a comprehensive approach to cyber risk management in organisations of varying scales. The work explored risk assessment methodologies, mitigation strategies, and cybersecurity best practices. It provided practical recommendations for developing security policies, staff training, and implementing technical information protection measures. Special emphasis was placed on the interplay between risk management and organisational business processes. The book became a valuable resource for executives and information security professionals.

The National Institute of Standards and Technology (NIST) standards were integral to cybersecurity efforts in the US and globally. For instance, NIST SP 800-115, Technical Guide to Information Security Testing and Assessment (2020), established a framework for information security testing and evaluation, assisting organisations in identifying vulnerabilities within their IT systems. The International Standard ISO/IEC 27400:2022 (E) (2022) provided guidelines for Internet of Things (IoT) solutions, addressing security and privacy risks associated with IoT devices and applications. It outlined principles and control measures to effectively mitigate these risks.

The ISO/SAE 21434:2021 (2021) standard focused on cybersecurity in the automotive industry, presenting requirements for cybersecurity risk management and a process framework to help original equipment manufacturers effectively communicate security-related risks. PCI Data Security Standard (PCI DSS) (2024) established security requirements for organisations handling credit card transactions, ensuring that sensitive payment data is protected against breaches and unauthorised access.

Additionally, the OWASP Top Ten 10 2025 (2024) annually published a list of the ten most critical web application security risks, serving as a vital resource for organisations to identify and mitigate vulnerabilities in their applications. The official source has announced the forthcoming release of the Top 10 Web Application Security Risks for 2025. Collectively, these standards contributed to a robust foundation for information security, guiding organisational efforts to protect sensitive data against an ever-evolving cyber threat landscape.

Beyond international standards, thematic case studies were a crucial component of research on this subject. Notably, B. Guttman *et al.* (2022) presented a case study outlining a digital evidence preservation model for criminal forensic institutions. This model emphasised compliance with legal admissibility requirements for court evidence. It included a comprehensive implementation guide, development plans, and outcome assessments, supporting institutions in aligning their digital evidence preservation practices with strategic objectives. The proposed model also enhanced the integrity and admissibility of digital evidence through long-term preservation methods based on the Open Archival Information System (OAIS) model.

Another relevant example was the analytical brief Preservation issues (n.d.), which discussed data preservation. This initiative illustrated the challenges associated with digital preservation, particularly in managing the interests of diverse stakeholders. The project highlighted the necessity of appointing a responsible officer to oversee digital preservation efforts, thereby clarifying responsibilities and ensuring effective leadership across institutional departments. This approach reduced ambiguity often surrounding preservation duties, fostering collaboration and stakeholder engagement. Strategic content sources enabled organisations to structure their own action plans for electronic document preservation, drawing on the experience of others.

The British Library Digital Preservation Strategy (2016) served as a significant practical example, outlining systematic approaches to preserving digital materials. The strategy examined various aspects of digital preservation, including the necessity of identifying components of digital works that required preservation and implementing measures to ensure their long-term survival. It emphasised the adoption of standards and practices facilitating digital content migration, as well as the importance of preserving both original hardware and software to access obsolete data formats (ISO 19005-4:2020, 2020).

A broader analysis of strategies to combat technological obsolescence can be found in the studies by S. Findlay (2018) and S. Findlay (2019), which explored several methods of information preservation. Among these were: migrating information to subsequent generations of technology, emulating the behaviour of legacy software, and maintaining original systems to run obsolete applications. Each strategy presents unique advantages and challenges, necessitating careful consideration of contextual factors to ensure effective long-term digital data preservation (Preservation issues, n.d.).

The Digital Preservation Strategy 2022-2026 (2022) became a foundational document that defined

key directions for the development of digital archiving at a national level. Of particular value was its comprehensive approach to addressing contemporary challenges in electronic records preservation, including issues of technological obsolescence, information security, and data accessibility. The strategy also established clear priorities and objectives to ensure the long-term preservation of the USA's digital heritage, making it an important benchmark for other institutions and organisations in developing their own approaches to digital preservation.

The risks associated with data loss underscored the need for robust data management strategies. In a study by J. McLeod (2008), the potential consequences of data loss were outlined, including financial and reputational damage due to the loss of business documentation or personal information. This highlighted the importance of implementing effective backup, redundancy, and recovery systems as part of any digital preservation efforts to mitigate risks – a point further emphasised by L.G. Paule (2023). Collectively, these thematic studies and strategic sources underscored the interdisciplinary nature of digital information preservation, stressing the significance of strategic planning, stakeholder engagement, and the implementation of best practices to ensure the longevity and integrity of digital information in accordance with international standards.

It was worth examining examples of best practices for effective digital data preservation, which have been crucial in ensuring the long-term accessibility and integrity of digital materials. Key methods included determining which materials should be preserved, ensuring data integrity, and applying technological solutions to combat obsolescence. Preservation strategies must account for the specific challenges posed by digital formats and rapid technological advancements, which may render certain formats obsolete – a point also discussed by S. Findlay (2018) and L.G. Paule (2023). An essential aspect of preservation has been the decision-making process regarding which materials to retain. This involves evaluating the strengths and weaknesses of data collections, particularly in contexts with limited storage capacity. Z. Teel (2024) noted that integrating artificial intelligence could streamline this decision-making process, helping responsible parties identify critical materials that might otherwise be overlooked due to human limitations in processing vast datasets.

The relationship between metadata and content has been fundamental to effective digital preservation. Metadata may be embedded within a digital object or stored separately, as in systems like the Open Archival Information System (OAIS), which proposed the use of "information packages" to combine content with descriptive preservation metadata (ISO 19005-4:2020, 2020). Proper documentation was crucial for maintaining the context and integrity of digital files, facilitating future access and use.

Maintaining a robust technological infrastructure has been essential for digital data preservation. This includes conducting annual audits to verify file integrity, updating storage media, and ensuring redundancy through backup replication. Techniques such as checksums can help verify that files remain unaltered over time (Paule, 2023; Preservation issues, n.d.). Furthermore, establishing a managed storage environment with multiple copies in geographically dispersed locations enhances protection against catastrophic data loss.

Forging partnerships between corporations and archives or libraries has been vital for sharing best practices and developing functional requirements for digital preservation. Such collaborations can lead to the creation of joint governance frameworks that address both immediate and long-term preservation needs in line with ISO 19005-4:2020 (2020). While existing guidelines often focus on the initial creation and capture of digital objects, it is equally critical to consider their ongoing accessibility. Continuous staff training is essential for effectively leveraging the capabilities of emerging digital preservation technologies. Professionals in this field must engage in ongoing career development to adapt to new challenges and methodologies. This entails attending workshops, courses, and exchanges, participating in professional networks, and staying informed about cutting-edge practices and technological advancements (Paule, 2023).

The future preservation of electronic records will be influenced by continuous technological advancements and the increasing complexity of digital records. As organisations grapple with managing vast volumes of data, a proactive approach to records management has become imperative. This approach highlights the importance of developing robust policies and systems to ensure the effective creation, capture, and management of records in alignment with organisational objectives, legal requirements, and regulatory frameworks – particularly ISO 15489-1:2016 (2016) and ISO/IEC 27001:2022 (2022). Consequently, based on the information presented, key trends in the development of electronic records can be outlined, as illustrated in Figure 1. The integration of artificial intelligence (AI) and machine learning into records management practices has created both opportunities and challenges. While AI can enhance efficiency through the automation of processes such as descriptive metadata generation, concerns persist regarding the potential displacement of records management professionals and the implications of over-reliance on automated systems. This has also been noted by P. Joseph *et al.* (2012) and A.L. Cushing & G. Osti (2023). As organisations seek to leverage AI, it is crucial to maintain a balance between technological advancements and the human expertise necessary for effective archival practice.

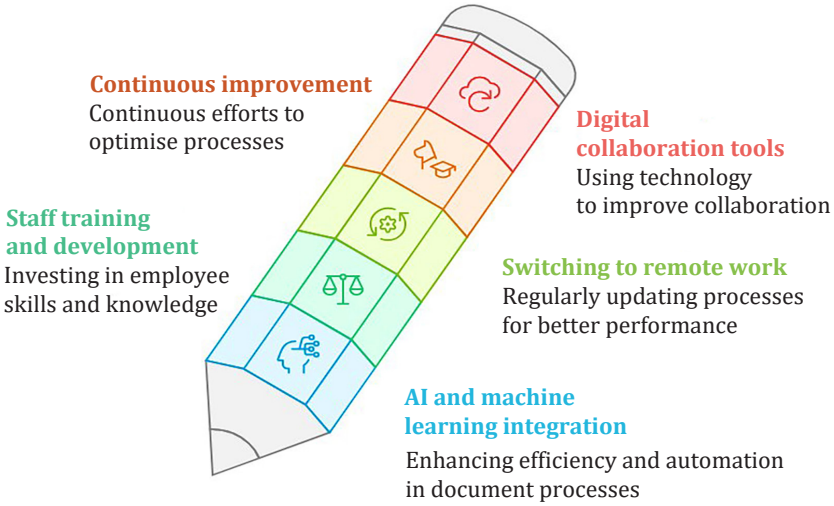

Figure 1. Trends influencing the development of electronic records management
Source: based on L.G. Paule (2023), Z. Teel (2024)

As the regulatory landscape evolves, organisations must remain cognisant of legislative and compliance requirements related to electronic records retention. A practice of continuous improvement, including regular review and updating of documented information management processes, will be essential for organisations to adapt to new regulatory demands while maintaining operational efficiency and adhering to international standards (Mancini, 2009; Biswas, 2023).

The shift to remote work and digital collaboration tools has introduced new challenges in electronic records preservation. Organisations must develop strategies that account for the diverse environments in which records are created and stored, ensuring usability across multiple devices without compromising functionality (Biswas, 2023). Furthermore, as data privacy concerns grow in significance, organisations must implement stringent measures to safeguard sensitive information from unauthorised access while complying with data protection regulations.

To effectively navigate the complexities of modern records management, organisations must invest in staff training and development. P. Joseph *et al.* (2012) noted that fostering knowledge-sharing and upskilling can empower records management professionals, ensuring their preparedness to operate within the evolving landscape of electronic records preservation. According to A.L. Cushing & G. Osti (2023), such investments in human capital will prove decisive as organisations strive to balance technological progress with the need for expert oversight in records management.

Preserving electronic records in accordance with international information security standards has presented organisations with numerous serious challenges. These challenges have been compounded by the rapid pace of digital transformation and the shifting compliance requirements landscape. One major issue has been data loss. As organisations increasingly transitioned to digital environments, the risk of losing valuable digital content became more pronounced. This has been emphasised in the works of I. Ismaili & R. Sülçevsi (2015) and L.G. Paule (2023). Data loss could occur due to various factors, including hardware failures, software corruption, accidental deletion, and cyberattacks. This underscored the necessity for robust backup and recovery strategies to ensure the longevity of digital records.

Another critical concern has been file format and software obsolescence. Over time, digital file formats and the software required to access them may become obsolete, complicating or even preventing access to archived records. Organisations must proactively engage in data migration processes to transfer information from obsolete formats into contemporary ones, ensuring continued accessibility. Compliance with ever-changing regulatory requirements also poses a significant challenge. International information security standards and industry regulations are continuously updated to address emerging threats and technologies (McLeod, 2008; Ismaili & Sülçevsi, 2015). Organisations must keep pace with these changes and adapt their information preservation strategies accordingly. Non-compliance with these standards may result in legal repercussions, financial penalties, and reputational damage.

Another issue has been the interoperability of diverse systems within and beyond organisational environments. Adherence to relevant standards facilitates regulatory compliance and ensures compatibility in digital preservation efforts across different platforms and sectors. Such interoperability is crucial for maintaining the integrity and accessibility of electronic records in the long term. According to B. Guttman *et al.* (2022), organisational challenges, such as insufficient resources and a lack of digital preservation expertise, may hinder

effective implementation. Developing and maintaining a digital preservation strategy requires substantial investments in technology, personnel, and training. Organisations must prioritise these efforts to safeguard their digital assets.

The management and preservation of electronic records have become critical for historical documentation and the protection of state and citizen interests, as noted by E. Zierau *et al.* (2021) and P. Biswas (2023). For instance, institutions must ensure the identification of vital records and their transfer to appropriate archival bodies for long-term preservation, such as the U.S. National Archives and Records Administration (NARA). Thus, preserving electronic records in line with international information security standards has entailed addressing challenges related to data loss, format obsolescence, regulatory compliance, system interoperability, and resource allocation (Fig. 2).

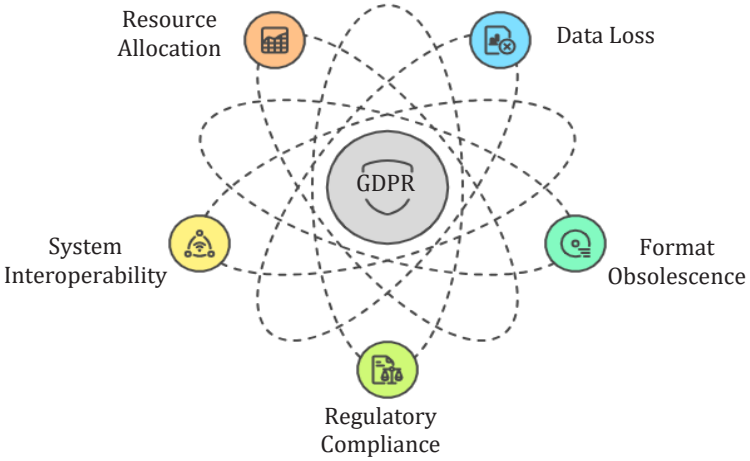

Figure 2. Challenges addressed by international standards
Source: based on E. Zierau *et al.* (2021), P. Biswas (2023)

By acknowledging these challenges and implementing comprehensive preservation strategies, organisations can safeguard their valuable digital content and ensure its accessibility for future generations. Specific strategies or best practices may be recommended to organisations to ensure the long-term preservation of electronic records in compliance with international information security standards. To guarantee the long-term preservation of electronic records, while adhering to international information security standards, organisations must adopt a holistic strategy encompassing both technical specifications and organisational policies. Several specific strategies and best practices were presented in Table 1.

Table 1. Strategies and best practices for electronic records preservation

No.	Strategy/Practice name	Description	Relevant standards & sources
1	Compliance with standards	The use of robust and up-to-date standards fundamental to the information industry. This facilitates access, retrieval, and exchange of digital resources, as well as their long-term preservation	ISO 14641:2018 (2018)
2	Comprehensive policies for records collection, storage, and access	Implementation of policies for the collection, storage, and access to electronic records, ensuring their integrity and traceability over extended periods. Such policies apply to records from diverse sources: scanned paper documents, converted analogue audio/video content, and digitally born content	I. Ismaili & R. Sülçevsi (2015), ISO 19005-4:2020 (2020)
3	Development of an operational model for digital preservation	Organisations should develop an operational model incorporating both industry-specific and universal standards to support digital preservation. Such a model ensures compliance and interoperability across different systems, while adherence to standards enables organisations to undergo auditing and certification	ISO 14641:2018 (2018)
4	Data administration and transfer policy	Establishment of a clear data administration and records transfer policy to ensure secure handling of electronic records throughout their lifecycle. The policy supports the transfer of records and databases in a manner that guarantees their long-term accessibility and integrity	B. Guttman *et al.* (2022)

Table 1. Continued

No.	Strategy/Practice name	Description	Relevant standards & sources
5	Regular auditing and updating	Conducting regular audits to ensure ongoing compliance with relevant standards and adaptation to evolving requirements. This includes monitoring updates to standards and integrating them into organisational policies and operational models	J. McLeod (2008), B. Guttman *et al.* (2022)
6	Education and training	Providing staff training on the importance of digital preservation and the specific policies and procedures they must follow	B. Guttman *et al.* (2022)

Source: developed by the authors

Thus, the study identified key standards ensuring the preservation of electronic records within the context of information security. Figure 3 presented the standards that safeguard information security in electronic records management, highlighting core provisions related to preservation, protection, and governance of electronic records.

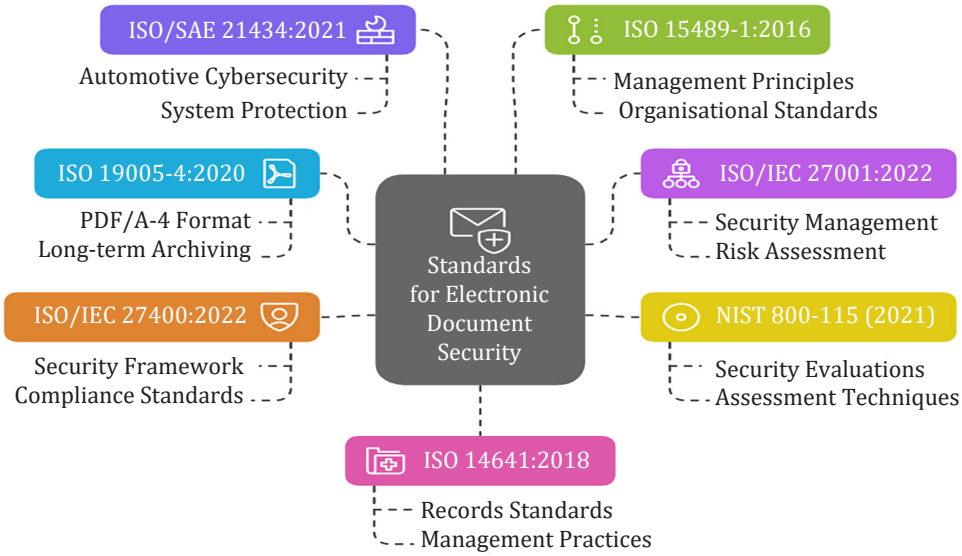

Figure 3. Key data of the electronic document security and management standard
Source: based on ISO 19005-4:2020 (2020), NIST SP 800-115, Technical Guide to Information Security Testing and Assessment (2020), ISO/IEC 27001:2022 (2022)

The capabilities of emerging technologies, such as artificial intelligence and blockchain, were designed to enhance the preservation of electronic documents in compliance with international information security standards. Blockchain technology has introduced a transformative approach to document management by ensuring the integrity, authenticity, and transparency of digital records. Blockchain employed a decentralised and immutable ledger system, where records were sequentially organised and cryptographically linked. This decentralised nature reduced the risk of unauthorised alterations and fraud, thereby preserving document integrity and traceability. The append-only nature of blockchain made it ideal for maintaining a verifiable record of document changes, ensuring compliance with standards such as ISO 14641:2018 (2018). Furthermore, blockchain can be integrated with existing document management systems to enhance their security and transparency. Organisations adopting blockchain for document management benefit from reduced risks associated with centralised data storage, as distributed ledger technology eliminates single points of failure (ISO 19005-4:2020, 2020).

Artificial intelligence (AI), including its subfields such as machine learning and natural language processing, can assist in various aspects of digital preservation management. AI technologies can automate document classification, indexing, and retrieval, thereby improving accessibility and efficiency. For instance, AI algorithms can analyse large volumes of documents to detect patterns and metadata, facilitating better organisation and search processes for required information or causal relationships within data. AI has also played a role in addressing privacy concerns by implementing automated redaction and anonymisation of sensitive information before documents are archived. Additionally, AI-based tools can support archivists by providing insights and recommendations, though human

oversight remains crucial to ensure ethical governance and contextual accuracy (Paule, 2023).

The integration of these technologies must align with established international information security standards. For example, the ISO 14641:2018 (2018) standard defined technical specifications and organisational policies for the collection, storage, and access of electronic documents to ensure their readability, integrity, and long-term traceability (Zierau *et al.*, 2021). Blockchain and AI can support compliance with these standards by ensuring that electronic documents remain authentic, unaltered, and accessible throughout their lifecycle. Thus, the combination of blockchain's immutable ledger and AI's automation capabilities can enhance electronic document preservation.

K. Sibil (2005) analysed the role of international descriptive standards ISAD(G) and ISAAR(CPF) in shaping a unified information space. The author examined the structure and application principles of these standards for archival description and the creation of standardised hierarchical metadata systems. The study highlighted mechanisms for ensuring compatibility between archival descriptions across institutions through the use of standardised approaches. This work contributed valuable insights into the fundamental principles of international standardisation in the archival field.

The authors S. Artamonova & L. Odynoka (2009) explored the role of national standards in unifying technological processes within reference libraries of archival institutions. The authors analysed practical aspects of applying standards to streamline document handling, optimise search systems, and ensure the preservation of collections. They also examined prospects for developing standardisation systems to integrate library and archival resources. The study demonstrated the interconnectedness of various branches of information activity within the context of standardisation.

L. Kyseleva (2012) examined European standards in archival science and records management within the framework of public administration. The author discussed key principles and requirements of European standards, their impact on the development of the archival sector, and governmental documentation management processes. The study included recommendations for implementing European approaches in Ukrainian contexts. S. Purser (2014) analysed the role of standards in cybersecurity and their practical application for protecting computer networks. The study reviewed key international and industry-specific standards, their interrelations, and evolution. It emphasised the importance of standardisation in developing effective incident detection and response systems. The work also examined future prospects for cybersecurity standards in light of emerging threats, offering valuable insights for professionals involved in designing and implementing information protection systems.

Scientists G. Kalinicheva & R. Romanovskyi (2015) investigated the harmonisation of international archival standards in Ukraine. The authors analysed challenges in adapting ISO standards to Ukrainian contexts, addressing improvements in regulatory frameworks for records management. The study provided an overview of achievements and future directions for national standardisation systems within Ukraine's integration into the European information space, with particular attention to practical implementation in Ukrainian archival institutions.

Data cybersecurity is also of critical importance. A. Davydiuk & O. Potii (2024) published a report as part of a series of national reports providing a comprehensive overview of cybersecurity governance across countries. Their research aimed to raise awareness of cybersecurity management in different national contexts, assisting countries in improving internal cybersecurity governance, promoting best practices, and fostering interagency and international cooperation. The report focused on NATO member states sponsoring the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). Each national report outlined the distribution of roles and responsibilities in cybersecurity among institutions, describing their mandates, tasks, and competencies, as well as interagency coordination. The report also contextualised the broader digital ecosystem of each country and outlined national cybersecurity strategy objectives to clarify the organisational approach within specific states.

Conclusions

The preservation of electronic documents was a critical challenge for modern organisations, requiring a comprehensive approach aligned with international information security standards. The study identified several key aspects of this issue. In particular, the primary challenges in electronic document preservation included technological obsolescence of data formats and storage media, complexities in electronic records management, data loss risks, and regulatory compliance requirements. Data loss emerged as a particularly critical issue, potentially leading to severe consequences for organisations, including financial losses and reputational damage. International standards played a foundational role in establishing effective electronic document management systems. These standards provided a structured approach to safeguarding information assets and ensuring long-term document preservation.

Successful electronic document preservation required the implementation of best practices, including regular material assessments, proper metadata management, reliable technological infrastructure, and continuous staff training. Collaboration between organisations and adherence to standardised preservation approaches were also essential. Future developments in electronic document preservation were linked to the

integration of cutting-edge technologies, such as AI and machine learning, which can significantly enhance documentation management efficiency. However, maintaining a balance between technological innovation and expert oversight remains crucial.

Ultimately, the study underscored the need for a proactive approach to electronic document management, encompassing clear policy development, investment in technological infrastructure, and continuous process refinement in response to evolving cyber threats and regulatory demands. Thus, effective electronic document preservation required a systemic approach combining technological solutions, organisational policies, and compliance with international information security standards.

Further research in this field should focus on examining the impact of emerging technologies on document preservation practices and developing innovative approaches to ensuring long-term access to electronic information.

Acknowledgements

None.

Conflict of Interest

None.

References

[1] Antonucci, D. (2017). *The cyber risk handbook: Creating and measuring effective cybersecurity capabilities.* Hoboken: John Wiley & Sons. doi: 10.1002/9781119309741.

[2] Artamonova, S., & Odynoka, L. (2009). National standards for archival and library affairs as a basis for unification of technological processes in the activities of scientific and reference libraries of archival institutions. *Studies in Archival Affairs and Documentation*, 17, 49-57.

[3] Biswas, P. (2023). ISO 27001:2022. Clause 7.5. Documented information. *Pretesh Biswas*. Retrieved from https://preteshbiswas.com/2023/12/24/iso-270012022-clause-7-5-documented-information/.

[4] British Library Digital Preservation Strategy. (2016). *British Library*. Retrieved from https://oc.ac.ge/pluginfile.php/649/mod_resource/content/0/BL_PresStrategy.pdf.

[5] Bullock, A. (1999). Preservation of digital information: Issues and current status. *Network Notes*, 60.

[6] Complete List of Cyber Security Standards. (n.d.). *AAT TEAM*. Retrieved from https://allabouttesting.org/complete-list-of-cyber-security-standards/.

[7] Cushing, A.L., & Osti, G. (2023). "So how do we balance all of these needs?": How the concept of AI technology impacts digital archival expertise. *Journal of Documentation*, 79(7), 12-29. doi: 10.1108/JD-08-2022-0170.

[8] Davydiuk, A., & Potii, O. (2024). *National cybersecurity governance: Ukraine.* Tallinn: The NATO Cooperative Cyber Defence Centre of Excellence.

[9] Digital Preservation Case Notes: Welsh Journals Online. (2010). *The National Library of Wales*. Retrieved from https://www.dpconline.org/docs/digital-preservation/case-study/450-casenotewelshjournals/file.

[10] Digital Preservation Coalition. (2024). Retrieved from https://www.dpconline.org/.

[11] Digital Preservation Strategy 2022-2026. (2022). *National Archives*. Retrieved from https://www.archives.gov/preservation/digital-preservation/strategy.

[12] Durniak, B., & Sabat, V. (2010). *Semantic protection of information in document management systems. Information technologies.* Lviv: Publishing House of the Ukrainian Academy of Printing.

[13] Findlay, C. (2018). Crunch time: The revised ISO 15489 and the future of recordkeeping. *Cassie Findlay*. Retrieved from https://surl.li/uctvmg.

[14] Findlay, C. (2019). Challenges and opportunities of the digital age: A recordkeeping perspective. *Cassie Findlay*. Retrieved from https://cassiefindlay.com/2019/05/08/challenges-and-opportunities-of-the-digital-age-a-recordkeeping-perspective/.

[15] Guttman, B., White, D.R., & Walraven, T. (2022). *Digital evidence preservation: Considerations for evidence handlers*. Gaithersburg: National Institute of Standards and Technology. doi: 10.6028/NIST.IR.8387.

[16] Guz, A. (2013). Evolution of the world standards of information security. *Information Security of the Person, Society and State*, 2, 8-12.

[17] Information security. (n.d.). *Digital Preservation Handbook.* Retrieved from https://www.dpconline.org/handbook/technical-solutions-and-tools/information-security.

[18] Institutional policies and strategies. (n.d.). *Digital Preservation Handbook.* Retrieved from https://www.dpconline.org/handbook/institutional-strategies/institutional-policies-and-strategies.

[19] Ismaili, I., & Sülçevsi, R. (2015). The era of electronic documents and the challenges facing their management. *Atlanti*, 25(1), 175-181. doi: 10.33700/2670-451X.25.1.175-181(2015).

[20] ISO 14641:2018. (2018). *Electronic document management – design and operation of an information system for the preservation of electronic documents – specifications*. Retrieved from https://www.bsbedge.com/standard/electronic-document-management-design-and-operation-of-an-information-system-for-the-preservation-of-electronic-documents-specifications-iso-14641-2018/ISO74338.

[21] ISO 15489-1:2016. (2016). *Information and documentation – records management. Part 1: Concepts and principles*. Retrieved from https://www.iso.org/obp/ui/en/#iso:std:iso:15489:-1:ed-2:v1:en.
[22] ISO 19005-4:2020. (2020). *Document management – electronic document file format for long-term preservation. Part 4: Use of ISO 32000-2 (PDF/A-4)*. Retrieved from https://www.iso.org/standard/71832.html.
[23] ISO/IEC 27001:2022. (2022). *Information security, cybersecurity and privacy protection – information security management systems – requirements*. Retrieved from https://www.iso.org/standard/27001.
[24] ISO/IEC 27400:2022 (E). (2022). *Cybersecurity – IoT security and privacy – guidelines*. Retrieved from https://cdn.standards.iteh.ai/samples/44373/cb2637b7641f43ed89851b00389b31c3/ISO-IEC-27400-2022.pdf.
[25] ISO/SAE 21434:2021. (2021). *Road vehicles – cybersecurity engineering*. Retrieved from https://www.iso.org/standard/70918.html.
[26] Joseph, P., Debowski, S., & Goldschmidt, P. (2012). Paradigm shifts in recordkeeping responsibilities: Implications for ISO 15489's implementation. *Records Management Journal*, 22(1), 57-75. doi: 10.1108/09565691211222108.
[27] Kalinicheva, G., & Romanovskyi, R. (2015). International standards in the field of archival affairs and management of documentary processes: Problems of harmonisation in Ukraine. *Archives of Ukraine*, 4, 54-73.
[28] Kyseleva, L. (2012). The definition of European standards in the field of the archived and office work. *Public Administration and Local Self-Government*, 4, 142-150.
[29] Mancini, J. (2009). 8 Steps of the ISO/TR 15489 records management methodology. *AIIM*. Retrieved from https://info.aiim.org/aiim-blog/newaiimo/2009/07/01/eight-steps-of-the-isotr-1548922001-records-management-program-implementation-methodology.
[30] Marulin, S. (2013). *Information technology of data exchange between the electronic document management system and the database of the information system.* (PhD dissertation, Odesa National Polytechnic University, Odesa, Ukraine).
[31] McLeod, J. (2008). A manager's guide to the long-term preservation of electronic document. *Records Management Journal*, 18(3). doi: 10.1108/rmj.2008.28118cae.002.
[32] NIST SP 800-115, Technical Guide to Information Security Testing and Assessment. (2020). *National Institute of Standards and Technology.* Retrieved from https://www.nist.gov/privacy-framework/nist-sp-800-115.
[33] OWASP Top Ten 2025. (2024). *OWASP*. Retrieved from https://owasp.org/www-project-top-ten/.
[34] Paule, L.G. (2023). ISO/IEC 27001 – the international standard for information security. *Official website of the European Union.* Retrieved from https://digital-skills-jobs.europa.eu/en/inspiration/resources/isoiec-27001-international-standard-information-security.
[35] PCI Data Security Standard (PCI DSS). (2024). *PCI Security Standards Council*. Retrieved from https://www.pcisecuritystandards.org/standards/pci-dss/.
[36] Preservation issues. (n.d.). *Digital Preservation Handbook.* Retrieved from https://www.dpconline.org/handbook/digital-preservation/preservation-issues.
[37] Publicly Available Standards. (2024). *International Organization for Standardization*. Retrieved from https://standards.iso.org/ittf/PubliclyAvailableStandards/.
[38] Purser, S. (2014). Standards for cyber security. In M.E. Hathaway (Ed.), *Best practices in computer network defense: Incident detection and response* (Vol. 35, pp. 97-106). Amsterdam: IOS Press Ebooks. doi: 10.3233/978-1-61499-372-8-97.
[39] Sabat, V. (2023). *Methodological bases of information technologies for document flow protection in hierarchical automated control systems*. (Doctoral dissertation, Ukrainian Academy of Printing, Lviv, Ukraine).
[40] Senchenko, M. (2022). To the problem of preservation of digital heritage. UNESCO Charter on the Preservation of Digital Heritage. *Bulletin of Book Chamber*, 12, 3-9. doi: 10.36273/2076-9555.2022.12(317).3-9.
[41] Sibil, K. (2005). International descriptive standards ISAD(G) and ISAAR(CPF) in the formation of a common information space. *Studies in Archival Affairs and Documentary Studies*, 13, 88-103.
[42] Teel, Z. (2024). Artificial intelligence's role in digitally preserving historic archives. *Preservation, Digital Technology & Culture*, 53(1), 29-33. doi: 10.1515/pdtc-2023-0050.
[43] UNESCO Charter on the Preservation of Digital Heritage. (2003). In *Intergovernmental council for the information for all programme.* Paris: UNESCO House. Retrieved from https://unesdoc.unesco.org/ark:/48223/pf0000229034.
[44] Zierau, E., McGovern, N., Goethals, A., Wu, C., & Schaefer, S. (2021). Digital preservation storage criteria and relevant standards: Latest development on the digital preservation storage criteria. In *17th international conference on digital preservation iPRES 2021* (article number 17). Beijing, China.

Питання збереження електронних документів у контексті міжнародних стандартів інформаційної безпеки

Людмила Філіпова
Доктор педагогічних наук, професор
Харківська державна академія культури
61057, Бурсацький узвіз, 4, м. Харків, Україна
https://orcid.org/0000-0003-0273-7922

Анна Шелестова
Кандидат наук із соціальних комунікацій, доцент
Харківська державна академія культури
61057, Бурсацький узвіз, 4, м. Харків, Україна
https://orcid.org/0000-0003-4866-1767

Анотація. Актуальність дослідження зумовлена стрімким розвитком електронного документообігу та зростаючою потребою у забезпеченні надійного збереження цифрових даних в умовах сучасних кіберзагроз та технологічних викликів. Мета дослідження полягала у комплексному аналізі проблем збереження електронних документів, розробці рекомендацій щодо впровадження ефективних систем управління електронною документацією відповідно до міжнародних стандартів. У дослідженні використано аналітичний метод для вивчення міжнародних стандартів інформаційної безпеки, системний підхід для розгляду процесів збереження документів як цілісної системи, порівняльний метод для аналізу різних підходів до збереження електронних документів, метод кейс-стаді при розгляді практичних прикладів впровадження систем електронного документообігу. Отримані результати продемонстрували критичну важливість врахування технологічного старіння форматів даних, складності процесів електронного документообігу та ризиків втрати даних. Розглянуто ключові аспекти управління та збереження електронних записів відповідно до міжнародних стандартів інформаційної безпеки. Наголошено на важливості впровадження комплексних стратегій для забезпечення довгострокового збереження цифрових документів. Було визначено шість основних стратегічних підходів: дотримання міжнародних стандартів; розробка комплексних політик збирання, зберігання та доступу до документів; створення операційної моделі для цифрового збереження; впровадження ефективної політики адміністрування та передачі даних; проведення регулярного аудиту та оновлення систем; забезпечення належної освіти та навчання персоналу. Було приділено увагу потенціалу новітніх технологій, таких як блокчейн та штучний інтелект, які можуть застосовуватися для підвищення ефективності збереження електронних документів. Блокчейн забезпечує цілісність, автентичність і прозорість через децентралізовану систему обліку, а технології штучного інтелекту оптимізують класифікацію, індексування та пошук документів, вирішують проблеми конфіденційності. Зазначено необхідність інтеграції цих технологій відповідно до встановлених міжнародних стандартів для забезпечення автентичності, незмінності та постійної доступності електронних документів. Практична цінність дослідження полягає у розробці рекомендацій щодо впровадження комплексу найкращих практик збереження електронних документів, включаючи регулярну оцінку матеріалів, управління метаданими та підтримку технологічної інфраструктури. Результати дослідження можуть бути використані організаціями для вдосконалення власних систем електронного документообігу та підвищення рівня інформаційної безпеки

Ключові слова: електронний документообіг; стандарти ISO; кібербезпека; цифрове збереження; управління метаданими; технологічна інфраструктура