Society. Document. Communication

Journal homepage: https://sdc-journal.com.ua/en
*Society. Document. Communication*, Vol. 10, No. 2, 8-21

***Article's History***: Received: 05.02.2025 Revised: 14.05.2025 Accepted: 23.06.2025

UDC 004.056.5:004.65:005.584

DOI: 10.69587/sdc/2.2025.08

# Information and analytical activity as a factor in enhancing information security and data reliability in electronic document management systems

**Oksana Pluzhnyk**
Doctor of Philosophy, Associate Professor
Hryhorii Skovoroda University in Pereiaslav
08401, 30 Sukhomlynskiy Str., Pereiaslav, Ukraine
https://orcid.org/0000-0001-8780-8288

**Vladyslav Duda***
Lecturer
Hryhorii Skovoroda University in Pereiaslav
08401, 30 Sukhomlynskiy Str., Pereiaslav, Ukraine
https://orcid.org/0009-0001-0048-4805

**Abstract.** The relevance of the study is driven by the growing need to employ information and analytical activity (IAA) as a key tool for ensuring information security and data reliability amid the active implementation of electronic document management systems (EDMS) in a digitalised society. This study aimed to comprehensively examine the role of information and analytical activity in enhancing information security and ensuring data reliability within electronic document management systems. The research employed methods of systems analysis, review of academic sources, and synthesis of information, as well as critical analysis of modern technical tools. The findings confirmed that IAA is a critically important factor in protecting information resources and maintaining data reliability in EDMS. Its integrated capacity for data collection, processing, analysis, and interpretation enables timely detection of threats, effective risk forecasting, control over the full document life cycle, and verification of authenticity. This facilitates not only prompt response to incidents but also the development of effective security policies that reduce the likelihood of data loss, distortion, or unauthorised access. The study identified key challenges, including a shortage of highly qualified specialists with interdisciplinary competences, difficulties in integrating heterogeneous systems, and legal and ethical constraints related to the protection of personal data and the transparency of analytical algorithms. The development prospects of IAA and EDMS are linked to the active integration of artificial intelligence and machine learning technologies for automated anomaly detection and threat forecasting, the use of blockchain solutions to ensure data immutability, and the application of Big Data tools to identify hidden patterns. Overcoming the outlined challenges and implementing innovative approaches will contribute to strengthening the reliability, security, and trustworthiness of digital documents. The practical value of the study lies in the possibility of applying its results to improve the efficiency of electronic document management systems through the integration of information and analytical tools aimed at ensuring information security and data reliability

**Keywords:** analytical systems; monitoring systems; security event analytics; information systems security; digital transformation; SIEM systems

***Suggested Citation:***
Pluzhnyk, O., & Duda, V. (2025). Information and analytical activity as a factor in enhancing information security and data reliability in electronic document management systems. *Society. Document. Communication*, 10(2), 8-21. doi: 10.69587/sdc/2.2025.08.

Copyright © The Author(s). This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/)

*Corresponding author

## Introduction

In the current context of digital transformation and rapid automation of business processes, electronic document management has become a foundation for the functioning of organisations in both the public and private sectors. However, as the volume of data created, transmitted, and stored in digital form increases, the issues of information security and data reliability become ever more acute. On a global scale, cyberattacks, interference in digital infrastructure, document falsification attempts, and the deliberate spread of disinformation are becoming increasingly widespread. This problem is particularly pressing for Ukraine, which operates under conditions of hybrid warfare and faces systemic pressure in the informational, cyber, and legal domains. Attempts to disrupt the work of state institutions, substitute or destroy official data, and undermine trust in digital governance tools are not isolated incidents but real threats to national security. In such an environment, information and analytical activity become a strategic tool that enables not only the detection of violations but also the forecasting of risks and the prevention of potential attacks.

A review of current academic research, both within Ukraine and in the international research domain, indicates growing attention to the issues of information and analytical activity under the conditions of digitalised document management. Contemporary studies focus not only on the technical aspects of integrating analytical tools into electronic document management systems (EDMS) but also on strategic questions of ensuring information security, data verification, and enhancing trust in electronic documents within complex digital ecosystems. Recent research highlights the transformation of information and analytical activity (IAA) in the context of digitalisation. N. Zozulya *et al.* (2025) emphasised the integration of advanced technologies – artificial intelligence, machine learning, big data, and cloud computing – into information analysis processes in both business and public administration. Particular attention is devoted to the use of cognitive technologies, neural networks, Natural Language Processing (NLP), and modern data visualisation platforms such as Power BI, Tableau, and Qlik Sense, which enhance automation and the timeliness of managerial decision-making. A related study by V. Voronkova *et al.* (2024) also examined the transformation of information and analytical support for organisational management through the introduction of digital technologies for real-time data collection, processing, and analysis. The authors emphasise the importance of integrating data from various sources, applying Big Data analytics to identify hidden trends, and employing cloud technologies to enhance management mobility. The practical value of such research lies in improving the efficiency of management processes, increasing the reliability of analytical information, and contributing to the sustainable development of organisations.

O.M. Odintsov *et al.* (2021) examined the legal and regulatory framework governing the functioning of EDMS and identified key challenges encountered during the implementation of such projects. Particular attention was given to the advantages of introducing electronic document management, including enhanced management efficiency, reduced bureaucratic workload, savings in time and resources, and the creation of a unified information environment. The study also addressed current technological trends and underscored the importance of a systematic approach to EDMS implementation, taking into account both external and internal influencing factors. In their article, S. Muminova *et al.* (2022) analysed the key security issues of electronic documents in the context of digitalised business processes, as well as modern protection technologies, including digital signatures and access control tools. The authors stressed the necessity of ensuring security throughout the entire document life cycle, highlighting six essential criteria: confidentiality, authorisation, accountability, integrity, authenticity, and non-repudiation. The proposed solutions enable the effective integration of protection mechanisms into corporate systems, ensuring the reliable preservation of data in both online and offline environments.

In the study by S. Sternad Zabukovšek *et al.* (2023), the connection between effective document life-cycle management and the increased reliability and security of data within digital systems is emphasised. Examining the influence of organisational maturity on the use of EDMS provides a deeper understanding of how information and analytical activity can contribute to improving control, transparency, and data reliability within the broader context of digital transformation in document management. When considering comprehensive control over the life cycle of an electronic document ensured by information and analytical activity (IAA), it is relevant to refer to the study by S. Kondratyuk & K. Palaguta (2021), which focuses on the selection and implementation of electronic document management systems in Ukraine. The research analyses current trends in the development of EDMS, proposes a system of criteria for software selection, and presents an algorithm for managerial decision-making throughout the entire document life cycle. This approach enables the alignment of analytical verification and document support (as described in IAA) with the stages of EDMS implementation and operation, thereby reducing risks and enhancing the efficiency of digital document management.

Existing academic research deepens the understanding of the transformations of information and analytical activity in the context of digitalisation, particularly in relation to ensuring cybersecurity and data reliability in electronic document management systems (EDMS). It demonstrates how organisations respond to hybrid threats, legal constraints, and the need for technological integration through the adoption of innovative

analytical solutions, automated verification systems, and predictive analytics, thereby underscoring the importance of strategic analytics for the stability of information systems and the development of proactive security policies. Despite this, the effective use of the potential of information and analytical activity to enhance information security and ensure data reliability in EDMS remains insufficiently explored. Most studies focus on the technical aspects of such systems, while the analytical component of risk management and document change control is often overlooked. As a result, analytical mechanisms within EDMS are either insufficiently integrated or applied primarily in a reactive mode, creating risks for business process continuity, organisational digital security, and trust in e-governance.

This study aimed to reveal the role of information and analytical activity in comprehensively enhancing information security and data reliability within electronic document management systems (EDMS). To achieve this aim, the following objectives were defined: to substantiate the theoretical foundations of information and analytical activity in the field of digital security; to identify key threats to data protection and reliability in EDMS; to analyse the potential of analytical tools for threat detection and risk forecasting; and to examine the practical aspects of IAA implementation. The scientific novelty of the study lies in the systematic generalisation of the role of IAA as an integrated mechanism for ensuring data reliability and cybersecurity in the context of digital transformation, taking into account current threats and technologies.

## Materials and Methods

The study adopted a comprehensive approach, combining theoretical, applied, and comparative methods with elements of empirical analysis aimed at a thorough assessment of the role of information and analytical activity (IAA) in ensuring information security and data reliability within electronic document management systems (EDMS). The factual basis of the research consisted of recent academic publications from the past three to five years, including studies by I. Aciobăniței *et al.* (2024), D.H. Awang Gani & I.K. Abdul Kadir (2024), and V. Somchenko *et al.* (2024). These studies addressed the practices and trends in the development of electronic document management systems (EDMS), the implementation of information and analytical technologies, risk management and cybersecurity assurance, as well as legal and organisational aspects of electronic document use, including issues of legal validity and document authenticity. The literature review made it possible to identify the key factors influencing the reliability, accuracy, and security of electronic documents, and to establish a foundation for further comparative and critical analysis of various approaches to the implementation of information and analytical mechanisms in the digital environment.

To achieve the stated aim, the study employed a set of scientific research methods that enabled a comprehensive analysis and systematic understanding of the examined processes. Systems analysis was used to investigate the structure of EDMS, its functional components, and its interconnections with IAA, allowing the identification of critical control and security points throughout the entire life cycle of electronic documents, as well as a clearer understanding of the interaction between analytical tools and digital platforms. Content analysis of academic sources made it possible to identify current trends in the development of information and analytical technologies, determine effective approaches to EDMS implementation, and assess their impact on data reliability and security. This enabled the identification of priority areas for improving existing systems. Critical analysis was applied to evaluate the effectiveness of specific analytical tools, including Security Information and Event Management (SIEM) systems, access control and user authentication tools, version control and electronic signature solutions, as well as data verification and audit modules. Comparative analysis allowed for the examination of different approaches to integrating IAA into EDMS, assessing their advantages and limitations, and determining optimal strategies for ensuring information security in organisational and technical processes.

The use of this set of methods ensured a comprehensive investigation of the role of IAA in electronic document management systems, integrating theoretical principles with the practical aspects of EDMS implementation, and forming evidence-based recommendations for improving the efficiency of information and analytical support, ensuring data reliability, and strengthening information security in modern digital organisations. This approach allows IAA to be viewed not merely as a tool for responding to threats but as a foundation for preventive risk management and strategic planning of information resource security.

## Results and Discussion

### Theoretical aspects of the study

Information and analytical activity represent a purposeful process of collecting, processing, analysing, and presenting information aimed at improving the quality of managerial decisionmaking, ensuring data reliability, and strengthening information security. The main objective of this process is the timely identification of potential threats, inaccuracies, or falsifications in electronic documents, as well as monitoring document flow logic, data integrity, and user behaviour within the system. The process of information and analytical activity involves several consecutive stages: from initial data collection (including automated extraction from documents and logs) to preliminary processing (normalisation, filtering, and cleaning), followed by analytical assessment (evaluation of reliability, detection of anomalies or logical inconsistencies), formulation of conclusions and recommendations,

and presentation of results in a decision-friendly format – such as reports, visualisations, or dashboards – as confirmed by O. Tkachenko & M. Humeniuk (2020). Thus, information and analytical activity serve as a strategic component in managing information security and data reliability within electronic document management systems (EDMS), enabling prompt responses to threats, minimising risks, and fostering trust in digital processes.

V.S. Politanskyi (2021) defined EDMS as a high-tech system of interrelated components functioning as a unified mechanism for electronic document exchange across computer networks. The author emphasised the importance of monitoring document movement and optimising management processes in public institutions, local authorities, and enterprises. The systems automate all stages of working with electronic documents – from input and registration to storage, viewing, searching, editing, execution control, and access management. In addition, the introduction of EDMS increases the efficiency of document handling, reduces printing and delivery costs, and contributes to enhancing the organisation's overall information culture.

A typical EDMS architecture includes several key components: access control, document registration and routing modules, a database for document storage, user interfaces, authentication tools (such as electronic signatures), and audit logs for recording user actions (Anggraini *et al*., 2024). Additional tools may include integration mechanisms with other IT systems – ERP, CRM, or state registers. The most vulnerable points in EDMS, where information security and data reliability risks arise, are associated with several factors (Han & Son, 2025). These include document transfer stages between nodes (risk of interception or substitution), user authentication (threat of credential compromise), data storage in databases (possibility of unauthorised modification or deletion), and the human factor (errors, misuse of access rights, or deliberate actions). Particular attention should be given to integration interfaces, which – if inadequately protected – may become channels for data leakage or manipulation.

As noted by A. Yasinska (2022), one of the current challenges remains the lack of a unified mechanism for electronic document exchange between different systems, which complicates their centralised storage in a single archive. The author notes that the anticipated implementation of the ASiC Standard is expected to ensure compatibility and enable businesses and government institutions to exchange electronic information efficiently. At present, exchange is possible through the System of Electronic Interaction (SEI), yet neither ASiC nor SEI is mandatory, which raises concerns among business leaders, as electronic document management providers are not required to guarantee compatibility between their systems. The findings of this study support these observations: an analysis of EDMS implementation practices revealed that the absence of unified standards indeed limits system integration, reduces the speed of data exchange, and complicates the maintenance of archive integrity, highlighting the necessity of implementing mandatory compatibility standards (System of Electronic Interaction of Executive Authorities (SEI EA), n.d.).

In an era of rapid information technology development and the transition to electronic document management, issues of information security and data reliability have become particularly pressing. As noted by D. Liudvenko *et al*. (2023), information and analytical activity "is a factor in enhancing information security and data reliability in electronic document management systems", emphasising its significance in the modern world. O. Fetisov (2024) observed that electronic document management systems substantially improve data protection by providing access control, transparency, and secure information storage. Through digital traces, restricted access for authorised personnel only, and the use of security labels, EDMS prevents the leakage of confidential information and loss of documents. Moreover, the transition from paper-based to electronic management minimises risks associated with physical storage. Thus, EDMS not only enhances information security but also optimises organisational operations in the face of increasing threats.

According to the authors of this study, data reliability in electronic document management refers to the characteristic of information that determines its ability to truthfully, accurately, and fully reflect the actual state of affairs, serving as a dependable basis for decision-making, legal actions, or managerial processes. In electronic document management systems (EDMS), reliability is particularly significant, as official actions, financial transactions, contract execution, and decisions with potential legal consequences are based on electronic documents. The key criteria for reliability are accuracy, completeness, timeliness, authenticity, and relevance. Accuracy denotes the correspondence of a document's content to the facts or events it describes, without distortion or errors. Completeness implies that all necessary components of the document are present, with no omissions, abbreviations, or missing elements. Timeliness refers to the alignment of data with the current state of affairs at the time of use – information should not be outdated or invalid. Authenticity indicates verified document origin, ensuring that it was created or signed by the declared entity without substitution or forgery. Finally, relevance refers to the appropriateness of the information for its intended purpose or query – it should be pertinent rather than random or extraneous (Nazarova, 2020). The presence of unreliable data in EDMS can have serious consequences, ranging from erroneous managerial decisions to legal conflicts, loss of trust, and organisational compromise. For example, incorrectly recorded details, an erroneous date, or a forged signature can call the validity of a contract into question or provoke legal disputes. Therefore, ensuring data reliability is not merely a

technical or organisational task but a strategic requirement, closely linked to accountability, legal risk, and reputational protection.

Electronic document management systems (EDMS) are information and communication platforms designed to automate the creation, processing, transfer, storage, and retrieval of electronic documents within an organisation or between entities. They support business process continuity, reduce information exchange times, and lessen reliance on paper-based media, as confirmed by D.H. Awang Gani & I.K. Abdul Kadir (2024). The results of this study also demonstrate that effective document management organisation directly reduces the risks of data loss or compromise and enhances the speed of managerial decision-making.

Information security in electronic document management systems is based on three core principles: confidentiality, integrity, and availability of information. These principles form the foundation for data protection and the uninterrupted operation of digital infrastructures (Osazuwa, 2023). Within the scope of this study, it was determined that adherence to these principles during the analytical processing of electronic documents improves the reliability of results and reduces the risk of logical errors or falsification. Confidentiality ensures that access to information is restricted to authorised personnel. In EDMS, this involves limiting document access rights, monitoring user accounts, and protecting transmitted data from interception. Breaches of confidentiality can occur through information leaks caused by phishing, malicious software, credential compromise, or internal threats – for example, dishonest employees (Fedoruk, 2024). In particular, under conditions of hybrid warfare and cyberattacks against Ukraine's state and corporate resources, the risk of theft of critically important documents is especially high. Integrity refers to maintaining the accuracy, completeness, and authenticity of data throughout the entire document life cycle. This is critically important for EDMS, as any unauthorised editing or falsification of documents can compromise their legal validity, result in financial losses, or create reputational risks. Typical threats to integrity include document modification without proper auditing, technical errors due to system failures, virus infections, or manipulation by malicious actors who have gained access to internal resources.

Availability ensures that documents can be accessed legally and without hindrance when needed. In EDMS, this means that users must be able to retrieve information quickly for work or decision-making. Threats to availability encompass both external attacks (such as DDoS attacks on servers) and internal failures – software errors, equipment malfunctions, inconsistent system updates, or the absence of backups. In contexts where document management supports critical processes (such as public administration, defence, or healthcare), loss of availability can have extremely serious consequences. Thus, the protection of confidentiality, integrity, and availability forms the foundation of secure electronic document management, with information and analytical activity playing a key role in the timely identification of threats, incident response, and reduction of the system's overall risk profile.

Accordingly, the authors of this study define information and analytical activity as a comprehensive set of processes aimed at collecting, processing, analysing, and evaluating information to ensure the reliability and security of electronic data. Within this research, information and analytical activity are treated as a tool that enables systematic verification, monitoring, and maintenance of data reliability in electronic document management systems by analysing the logical structure of documents, verifying sources, cross-referencing information with internal and external registers, and recording potential deviations requiring attention. In this way, data reliability is regarded as the cornerstone of the entire digital document management ecosystem.

**The role of information and analytical activity in enhancing information security in electronic document management systems**

Information and analytical activity (IAA) play a central role in monitoring the security of electronic document management systems (EDMS) and identifying potential threats before they escalate into actual incidents. Effective IAA in this context relies on the continuous collection, processing, and analysis of large volumes of data generated during EDMS operation, including log files, event journals, user actions, and metadata related to document workflows. In particular, log analysis forms the basis for detecting both technical and behavioural anomalies. IAA enables the systematisation of events – such as system logins, access-rights changes, document edits, and signings – and the identification of patterns that may indicate suspicious activity. Examples include repeated login attempts from different IP addresses, access to documents outside working hours, or edits made by users without the necessary authorisation (Martín *et al*., 2021).

Another important tool is the analysis of user behavioural patterns. Machine learning algorithms can be used to create profiles of "normal" activity for each user or department. Deviations from these patterns – such as a sudden increase in the volume of downloaded documents or access to unusual categories of files – are automatically flagged as potential indicators of compromise or internal threats (Shi *et al*., 2020). Additionally, IAA allows for the monitoring of anomalous information flows, including atypical document transfer routes, data duplication, and attempts to export or import files without authorisation via integration interfaces. This is particularly critical during external cyberattacks, where disruption of document workflow logic can be one of the earliest signs of intrusion (Perapu, 2025).

Overall, information and analytical activity provide the foundation for proactive cyber protection of EDMS.

It enables the system not only to respond to threats that have already occurred but also to detect potential vulnerabilities at an early stage, preventing data loss, integrity breaches, and business process interruptions. When combined with visualisation tools, reporting mechanisms, and early warning systems, IAA establishes an intelligent layer of information security management within electronic document management. Risk forecasting in electronic document management systems (EDMS) is a crucial aspect of information and analytical activity, enabling not only a reactive response to information security incidents but also their proactive prevention by assessing both the likelihood and potential impact of such events (Alotaibi, 2023). This significantly enhances the system's overall resilience to threats and supports a proactive approach to information security management.

One of the key tools in this process is the analysis of historical incident data. By examining accumulated logs, failure reports, attempts at unauthorised access, internal breaches, or user errors, recurring patterns, typical vulnerabilities, and temporal or behavioural trends can be identified (Landauer *et al*., 2025). For instance, statistical analysis may reveal that the number of violations rises sharply during certain periods of the year – such as during staff changes or reporting cycles – providing a basis for strengthening controls during these times. Predictive models are then built using these data – algorithms that employ machine learning or mathematical modelling techniques to assess risk levels according to defined indicators. For example, if the system records a user changing IP addresses, altering access rights, and downloading large volumes of documents, this combination of factors may be interpreted as a high risk of an internal threat. Predictive models allow such situations to be automatically classified as critical and trigger appropriate response protocols. Furthermore, IAA is used to evaluate the potential consequences of incidents, which is equally important as assessing their probability. For example, a breach of clients' personal data or the falsification of a contract can have varying degrees of impact on an organisation, ranging from reputational damage to legal liability. Modern analytical systems, therefore, take into account not only the occurrence of an incident but also the associated risk value – reputational, financial, or legal. As a result, risk forecasting based on IAA enables organisational leadership to make informed decisions regarding the allocation of security resources, the refinement of access policies, software updates, staff awareness training, and other preventative measures. In this way, analytics becomes the foundation for strategic security management in a digital document environment (Levandovska, 2023).

According to the authors of this study, analytical data collected and processed through information and analytical activity (IAA) constitute a critical basis for developing and continuously improving information security policies and procedures in electronic document management systems (EDMS). By leveraging these data, policies become actionable tools for risk management and the maintenance of data integrity rather than mere declarative documents. The analysis of incidents and vulnerabilities allows the formulation of evidence-based access policies for electronic documents, defining which categories of users should have access to specific types of documents, how authenticity checks should be conducted, and how misuse of access rights can be prevented. For instance, if analytical systems detect a high incidence of issues linked to excessively broad access rights, policies can be adjusted according to the principle of least privilege. IAA also helps determine the need for detailed backup and data recovery procedures (Tekin *et al*., 2023). Based on statistics regarding data loss or corruption, as well as assessments of potential damage, it is possible to determine the appropriate frequency for creating backups, identify which components of an EDMS are critical to business processes and require enhanced protection, and establish the most reliable storage formats and repositories.

Analytics also plays a crucial role in shaping incident response policies. By modelling scenarios and analysing past response times to security events, clear procedures can be developed for staff to follow when breaches are detected – specifying who should be notified, which resources must be isolated, and which actions should be recorded. Additionally, user behaviour analysis forms the basis for internal digital hygiene regulations, such as the frequency of password changes, requirements for multi-factor authentication, and restrictions on the use of personal devices (Noori & AlHashimi, 2023). IAA enables these rules to be tailored to actual organisational needs and risks, rather than merely adhering to general standards.

Within the scope of information and analytical activity, key functions include the collection of relevant data, its systematic organisation, analytical processing, and subsequent synthesis, interpretation, and forecasting based on the findings. As noted by V. Savchuk & V. Derii (2023), this study emphasises the importance of monitoring deviations from standard procedures within the document management system, identifying logical errors in the content or structure of documents, and detecting potential signs of falsification. The predictive component, highlighted by G. Sichkarenko & S. Yaremko (2022), is also supported in this study, demonstrating the effectiveness of modelling potential risk scenarios and implementing proactive cybersecurity measures. Analytical data provides feedback between the actual state of information security and the organisation's regulatory framework. Consequently, policies and procedures not only comply with current legislation and international standards but also dynamically adapt to changes in threats, technologies, and organisational processes.

**Ensuring data integrity through information and analytical activity**

Information and analytical activity play a key role in ensuring data integrity within electronic document management systems (EDMS), particularly through the verification and validation of electronic documents. These processes guarantee that the data processed, stored, and transmitted within the system is authentic, complete, unaltered, and compliant with established standards. Methods for ensuring data integrity in electronic document management systems include electronic signature verification to confirm document authenticity, hashing to monitor integrity and detect modifications, timestamping to record the moment of creation or signing, audit logging to trace the history of changes and access, and behavioural analysis of users to identify anomalies and unauthorised actions. Together, these measures provide comprehensive protection and control over information (Table 1).

**Table 1.** Methods for ensuring data integrity in EDMS

| Method | Purpose | Example of use |
|---|---|---|
| **Electronic signature verification (ESV)** | Confirms the authenticity and integrity of a document by verifying the sender's digital signature | Checking electronic signatures in documents using certificates from trusted authorities |
| **Hashing (Checksum, Hash functions)** | Creates a unique digital fingerprint of a document to monitor integrity and detect changes | Detecting unauthorised modifications to files after editing or transmission |
| **Timestamping** | Records the exact time a document is created or signed to protect against date manipulation | Protecting electronic documents from falsified dates and altered timestamps |
| **Audit logging** | Tracks and records all changes, operations, and access to documents to ensure transparency and control | Logging the history of edits, access, and deletions of documents in an EDMS |
| **User behaviour analysis** | Identifies anomalies in user activity by analysing deviations from normal behaviour | Detecting unauthorised access attempts or atypical document operations |

**Source:** J. Kim *et al.* (2019), A. Saepulrohman & A. Ismangil (2021), V. Semchenko *et al.* (2024), I. Aciobăniței *et al.* (2024), D.H.A. Gani *et al.* (2024)

Verification of electronic documents involves confirming their authenticity – that is, ensuring the document was genuinely created by the stated author and has not been falsified or altered by third parties. In this context, one of the main tools is the qualified electronic signature (QES) (Somchenko *et al.*, 2024), which provides legal validity, verifies the identity of the signatory, and records their consent to the content of the document. IAA is used for the automated verification of the validity of QES, in particular by cross-checking signature certificates against trusted authority databases (Aciobăniței *et al.*, 2024). Document integrity is ensured through checksums (hash functions) – algorithms that generate a unique digital fingerprint of the document. The analytical system compares the checksum at the time of creation with the current value; any alteration, however minor, changes the hash and signals a loss of integrity. Such mechanisms allow the detection of unauthorised edits or data corruption during storage or transmission (Saepulrohman & Ismangil, 2021).

Timestamps represent another critical element, recording the precise moment a document is created or signed. This prevents backdating or manipulation of document chronology. Information-analytical tools verify the validity and consistency of timestamps and cross-check them against system event logs to identify anomalies. Audit logging in electronic document management systems provides version control, records user actions, and safeguards access to documents. Although initially considered statistically minor, subsequent bootstrap analysis confirmed its significant impact on overall EDMS effectiveness, highlighting the key role of the audit trail in enhancing transparency and manageability of document processes (Gani *et al.*, 2024).

User behaviour analysis (User Behaviour Modelling) is one of the most effective methods for detecting insider threats in digital systems, particularly within electronic document management systems. The approach involves creating models of typical user behaviour based on collected activity data and identifying deviations that may indicate potential misuse or unauthorised actions (Kim *et al.*, 2019). Together, these methods form a comprehensive framework for document verification and validation in EDMS, where information-analytical activity provides not only automated checks of formal indicators of authenticity but also analytical evaluation of the context in which documents are used. This enables the timely detection of suspicious activity and minimises the risk of legal or organisational consequences. Consequently, IAA becomes a cornerstone of trust in digital documents within a dynamic information environment.

Information-analytical activity (IAA) ensures oversight of the entire lifecycle of an electronic document in electronic document management systems (EDMS), from creation through to archiving or disposal. At each stage, IAA performs monitoring, analysis, verification, and event recording, thereby guaranteeing the integrity, authenticity, and relevance of the document throughout its existence (Chaikovska & Stolyarchuk, 2018). Analytical tools within EDMS conduct detailed checks at the creation stage – recording the source of initiation, the legitimacy of the author's actions, the presence of an electronic signature, compliance with templates and metadata, and establishing log control points required

for subsequent auditing. During the editing and review process, the system tracks all changes, generates a version history, records the chronology of actions, checks compliance with policies, and identifies suspicious activity, including unauthorised edits or procedural violations. This is supported by recent studies (Laue *et al*., 2022), which describe SIEM architectures with advanced analytical capabilities, including the automatic generation of incidents based on logs.

At the approval and signing stage, IAA verifies the validity of qualified electronic signatures, the accuracy of timestamps, and the users' role-based permissions. Contextual analysis – identifying who signed the document, when, and from which device – helps prevent fraud. Similar approaches are confirmed by studies on AI-enhanced audit processes (Binh, 2025), which support transparency, traceability, and regulatory compliance. During storage and use, analytical tools monitor access, frequency of use, participation in transactions, and content integrity. Continuous monitoring enables timely responses to potential data leaks or unauthorised modifications, a functionality described in research on intelligent SIEM solutions with big data analytics and the generation of "smart" alerts (González-Granadillo *et al*., 2021).

In the archiving or destruction stage, IAA records the completion of the document's lifecycle, verifies that secure storage or complete deletion procedures have been followed, and ensures a comprehensive audit trail of all document-related actions. Thus, information and analytical activity create a continuous digital trail of a document, allowing its history to be reconstructed, its authenticity to be verified at any stage, and the legitimacy of all participants' actions to be demonstrated. This is a key requirement for both maintaining information security and preserving the legal validity of electronic documents (Zhou & Zhang, 2024).

Audit and change monitoring are integral components of information and analytical activity in electronic document management systems (EDMS), as they ensure transparency, control, and the ability to conduct retrospective analysis of all actions related to electronic documents. These processes aim to record every modification to a document, as well as to detect and prevent unauthorised interventions or breaches of security policies (Jannah *et al*., 2023). A central tool in this context is the audit log, which automatically records all document-related actions: creation, editing, approval, signing, access, movement, archiving, or deletion. For each event, metadata are captured, including date and time, user, type of action, and IP address or device used for access. This enables precise identification of the individual responsible for each change and allows the complete chronology of the document's lifecycle to be traced (What is an audit trail…?, n.d.).

Analytical tools integrated into the EDMS analyse audit logs to detect deviations from normal behaviour or violations of established procedures. For example, if a document is modified outside the standard approval process or accessed by a user without the appropriate permissions, the system generates an alert or automatically initiates an investigation. Such mechanisms are particularly important for organisations where documents carry legal weight or contain sensitive information. Moreover, audit results can be used to produce analytical reports on document security, detailing the number of changes, user access levels, and the most frequent anomalies. This enables potential weaknesses in information policies to be identified, threats to be addressed promptly, and rules for document handling to be improved (Walters, 2025).

The authors concur with the conclusions of L. Bozhuk & T. Kurchenko (2023), who identify IAA as a critically important factor in the stability and effective functioning of public institutions, where information and analytical activity generate secondary informational outputs such as reports, briefings, or forecasts. In comparison with their findings, the results of this study confirm this role and further demonstrate the practical significance of IAA in EDMS for detecting internal risks and anomalies in document flows. As noted by L.A. Kovalska (2021), IAA comprises a set of processes for collecting, searching, processing, transmitting, and using information to ensure effective management, combining the informational aspect (data accumulation and systematisation) with the analytical aspect (in-depth processing of information using logical reasoning and technical tools). The results of this study support L.A. Kovalska's conclusions regarding the key role of IAA in the digitalisation of document management. Furthermore, this research extends L.A. Kovalska's approach by demonstrating that the use of modern IT tools (SIEM, DLP, Big Data) not only enables the systematic organisation and storage of data but also enhances its reliability, forecasts potential threats, and provides comprehensive protection for electronic documents. Consequently, audit and change-monitoring processes ensure a high level of transparency and accountability in handling electronic documents, reduce the risks of forgery or falsification, and create an evidential basis for safeguarding organisational interests in the event of incidents.

**Tools and methods of IAA for enhancing security and data integrity**

The integration of information and analytical activity (IAA) into electronic document management systems (EDMS) is implemented according to the system model and type of organisation, aiming to enhance information security and data integrity. In government institutions and local authorities, a centralised EDMS model with distributed access is employed, where Security Information and Event Management (SIEM) systems monitor access to registries and electronic files in real time, alerting to attempts at unauthorised document modification (Koshara & Bakalo, 2023). Simultaneously, DLP solutions

control the transmission of confidential documents between departments and external partners, while Big Data analytics help identify bottlenecks in decision-making processes, recurring errors, and suspicious delays.

In commercial enterprises, modular integration of EDMS with CRM and ERP systems enables monitoring of access to financial documents and contracts, prevents the copying of confidential information, and forecasts risks for financial operations through Big Data analysis. In universities and research institutions, a decentralised EDMS model allows faculties to manage electronic documents autonomously, while SIEM systems control access to research articles and reports, DLP solutions restrict the forwarding of materials, and Big Data analytics track document access frequency to detect potential leaks or copyright violations (Kotwal, 2024).

For example, the Ukrainian service Vchasno.EDO automatically verifies electronic signatures, protects keys and passwords, scans documents for viruses, and stores them in a secure cloud archive (Amazon S3), providing multi-level access control (Vchasno, n.d.). Its clients include over 1,000,000 companies, such as Nova Poshta, Glovo, Uber, Monobank, and others (Vchasno group, n.d.). At the international level, solutions based on Splunk Enterprise Security demonstrate high efficiency in SIEM monitoring, reducing false alarms by up to 90%, accelerating incident response, and automating audits, making them one of the leading tools in IAA systems (Splunk, n.d.).

Banks and financial institutions employ multi-tiered EDMS models with role-based access, where SIEM systems monitor operations involving client and internal documentation, DLP solutions restrict the export and printing of confidential information, and Big Data analytics detect suspicious transactions and anomalous employee activity (Le *et al*., 2025). The integration of IAA technological tools – SIEM, DLP, Big Data analytics, cryptographic methods, and data visualisation – enables a comprehensive approach to the control, monitoring, and protection of information resources across various EDMS models, enhancing system resilience to both internal and external threats and supporting informed decision-making. Information and analytical activity (IAA) within electronic document management systems (EDMS) relies heavily on a suite of modern tools and methods (Table 2) that strengthen information security and data reliability.

**Table 2.** Tools and methods of IAA for ensuring security and data reliability in EDMS

| Tool/Method | Function in IAA | Relation to security and reliability |
|---|---|---|
| **SIEM (Security Information and Event Management)** | Collection, monitoring, and correlation of security events in real time | Detection of incidents, facilitation of investigations, support for audits |
| **DLP (Data Loss Prevention)** | Control and prevention of unauthorised leakage of confidential information | Protection against disclosure of critical data, preservation of confidentiality |
| **Big Data / Data Mining** | Analysis of large volumes of heterogeneous data to identify hidden patterns | Risk forecasting, anomaly detection, enhancement of analytical reliability |
| **Cryptography** | Data encryption, digital signatures, key generation | Ensures integrity and authenticity, protects against unauthorised access |
| **Analytics visualisation** | Graphical representation of data to support decision-making and trend detection | Assessment of information security status, verification of reliability based on visual patterns |

**Source:** P. DupinBryant & D. Olsen (2014), K. Kaur *et al.* (2017), G. González-Granadillo *et al.* (2021), J. Schwenk (2022), C. Cavallaro *et al.* (2023)

One of the key components is Security Information and Event Management (SIEM) systems, which enable the real-time collection, correlation, and analysis of security events. These systems facilitate the detection of incidents, the analysis of user behaviour patterns, the automation of threat response, and the generation of reports for subsequent auditing. For instance, in a simulated institutional scenario, a SIEM system could automatically record attempts to access documents outside working hours, alerting analysts to a potential risk and initiating an access review (González-Granadillo *et al*., 2021).

To prevent the leakage of confidential information, Data Loss Prevention (DLP) systems are employed (Kaur *et al*., 2017). They monitor the movement of data across networks, block unauthorised attempts to copy or transmit documents, and ensure compliance with organisational security policies (Herrera Montano *et al*., 2022). In a practical scenario, this might involve automatically blocking the sending of a document containing personal data to an external email address while simultaneously recording the incident for further analysis. The large volume of data generated within an EDMS necessitates the use of Big Data and Data Mining methods (Cavallaro *et al*., 2023). These tools allow hidden patterns, trends, and anomalies to be identified, which may indicate fraud, unauthorised access, or other threats. For example, analysing document access logs with Big Data techniques can reveal repeated atypical actions by a specific user, signalling a potential security breach.

Cryptographic methods ensure the authenticity and integrity of documents. Information and analytical activity support the selection and implementation of encryption algorithms, hashing, and electronic signatures, guaranteeing that documents remain unaltered after signing and verifying the signatory's identity (Schwenk, 2022). To enhance decision-making efficiency, analysts make extensive use of statistical methods and data visualisation. Graphs, charts, heat maps, and other

visual tools help structure and simplify the interpretation of complex information regarding security status, data integrity, and identified risks. In a practical scenario, a manager can clearly see highrisk areas and make timely decisions regarding additional controls or access restrictions (DupinBryant & Olsen, 2014).

Thus, the integration of these tools and methods within information and analytical activity establishes an effective mechanism for comprehensive control, monitoring, and protection of information resources in an EDMS. SIEM systems enable the rapid detection of incidents and the auditing of security events; DLP solutions prevent the leakage of confidential information; Big Data and Data Mining analytics reveal hidden threats and forecast risks; cryptographic tools guarantee the integrity and authenticity of documents; and data visualisation facilitates swift and wellinformed decision-making. This approach enhances the resilience of an EDMS against internal and external threats while demonstrating the practical applicability of these technologies in realworld scenarios.

The analysis identified several optimal strategies for ensuring information security in an EDMS. Firstly, a multi-level access control strategy that combines user authentication, differentiated permissions, and activity monitoring. Secondly, a strategy of end-to-end document verification using electronic signatures, cryptographic algorithms, and data integrity checking modules. Thirdly, an analytical monitoring strategy for security events, based on the integration of SIEM and DLP solutions to enable timely incident detection and prevent information leaks. Fourthly, a predictive analytics strategy employing Big Data and Data Mining to identify hidden risks and develop response models for potential threats. Finally, a strategy for a transparent document lifecycle, encompassing version control, audit of user actions, and data visualisation to maintain trust in electronic document management.

The article by S. Paliy (2022) highlights the significance of information and analytical activity (IAA) in ensuring information security and data integrity within electronic document management systems, aligning closely with the objectives of this study. In particular, the article emphasises IAA as a tool for timely threat detection, risk forecasting, and data verification in digital systems – key aspects addressed in the present research. S. Paliy (2022) also underscores the importance of integrating IAA with other technologies to enhance the reliability and security of information resources and notes its critical role in guaranteeing data integrity and safeguarding information systems amid digital transformation. The article by V. Zahumenna & O. Kuzmenko (2022) and the present study both examine the development of information and analytical activity (IAA) as a discipline foundational to enhancing information security. However, this study focuses on the application of IAA to improve data integrity within electronic document management systems (EDMS), whereas V. Zahumenna & O. Kuzmenko highlight the role of IAA in the context of education and professional development, which is essential for the effective implementation of security tools in digital systems. Both studies confirm the importance of IAA in ensuring the reliability of data in digital environments.

The integration of modern information and analytical activity tools into electronic document management systems enhances both security and data integrity. The use of SIEM, DLP, Big Data analytics, cryptographic methods, and data visualisation enables the detection of incidents, prevention of information leaks, risk forecasting, verification of document integrity, and informed decision-making. This comprehensive approach establishes multi-layered protection, a transparent document lifecycle, and increases the resilience of EDMS to both internal and external threats.

## Conclusions

The findings of this study confirm that information and analytical activity (IAA) is a critical factor in ensuring information security and data integrity within electronic document management systems (EDMS). Such systems not only automate management processes but also safeguard information through built-in mechanisms for access control, auditing, and authentication. Maintaining an appropriate level of information security relies on the principles of confidentiality, integrity, and availability, the balance of which is essential for business continuity and the development of trust in digital technologies. A systematic approach to the collection, processing, analysis, and evaluation of data within EDMS ensures its reliability, positioning IAA as a key component of an effective and secure digital infrastructure.

The information and analytical activity serve as a crucial mechanism for enhancing the information security of EDMS, providing monitoring, detection, and early-stage threat forecasting. The analysis of logs, user behaviour, and information flows enables the identification of anomalies and internal risks, supporting a proactive security posture. Predictive models based on incident data help assess the likelihood of threats and the potential scale of their consequences, thereby increasing system resilience. Analytical data inform the refinement of access policies, backup procedures, incident response strategies, and digital hygiene practices. IAA allows policies to be adapted to the actual security context, maintains the integrity of electronic documents, and strengthens trust in digital document management.

Within EDMS, information and analytical activity ensure the reliability of data throughout the entire lifecycle of an electronic document. Verification of electronic signatures, integrity checks using hash functions, timestamping, audit logging, and user behaviour analysis together form a comprehensive mechanism for information protection. IAA ensures the authenticity and legal validity of documents, detects unauthorised modifications, guarantees transparency and access control, prevents

internal threats, and creates a complete digital trail of each document, enabling the reconstruction of its history and verification of the legitimacy of all actions. Consequently, IAA underpins the reliability, security, and legal significance of electronic documents, enhances trust in EDMS, and minimises the risk of violations or falsifications.

The tools and methods of information and analytical activity within EDMS provide multi-layered information protection and data integrity. SIEM systems detect incidents, correlate events, and support auditing, thereby enhancing transparency and control. DLP solutions prevent the leakage of confidential information and ensure compliance with security policies. Big Data and Data Mining enable the analysis of large datasets, the identification of anomalies, and the forecasting of potential threats. Cryptographic measures guarantee the integrity and legal significance of documents, while data visualisation facilitates timely and informed decision-making. The integrated application of these tools increases the resilience of EDMS against threats and strengthens user trust. A promising direction for future work is the standardisation and expansion of IAA capabilities within electronic document management systems.

## Acknowledgements

None.

## Funding

None.

## Conflict of Interest

None.

## References

[1] Aciobăniței, I., Arseni, Ș.-C., Bureacă, E., & Togan, M. (2024). A comprehensive and privacy-aware approach for remote qualified electronic signatures. *Electronics*, 13(4), article number 757. doi: 10.3390/electronics13040757.

[2] Alotaibi, E.M. (2023). Risk assessment using predictive analytics. *International Journal of Professional Business Review,* 8(5), article number e01723. doi: 10.26668/businessreview/2023.v8i5.1723.

[3] Anggraini, D., Adi, K., & Suseno, J.E. (2024). Electronic document management systems implementation across industries: Systematic analysis. *Indonesian Journal of Electrical Engineering and Computer Science*, 36(1), 264-273. doi: 10.11591/ijeecs.v36.i1.pp264-273.

[4] Awang Gani, D.H., & Abdul Kadir, I.K. (2024). Electronic document management: The essence of effective modern organisation. *Journal of Information and Knowledge Management*, 14(2), 77-85. doi: 10.24191/jikm.v14i2.4472.

[5] Binh, N.T.T. (2025). Transforming auditing in the AI Era: A comprehensive review. *Information*, 16(5), article number 400. doi: 10.3390/info16050400.

[6] Bozhuk, L., & Kurchenko, T. (2023). Information and analytical support for the activities of local governments in Ukraine. In *V international scientific and practical conference "Scientific practice: Modern and classical research methods"* (pp. 73-76). Boston, USA. doi: 10.36074/logos-22.12.2023.018.

[7] Cavallaro, C., Cutello, V., Pavone, M., & Zito, F. (2023). Discovering anomalies in big data: A review focused on the application of metaheuristics and machine learning techniques. *Frontiers Big Data*, 6, article number 1179625. doi: 10.3389/fdata.2023.1179625.

[8] Chaikovska, O., & Stolyarchuk, I. (2018). Analysis of e-document management systems in Ukraine and criteria for their selection. *Technology Audit and Production Reserves*, 3(2(41)), 18-24. doi: 10.15587/2312-8372.2018.134120.

[9] Dupin-Bryant, P.A., & Olsen, D.H. (2014). Business intelligence, analytics and data visualization: A heat map project tutorial. *International Journal of Management & Information Systems (IJMIS)*, 18(3), 185-200. doi: 10.19030/ijmis.v18i3.8705.

[10] Fedoruk, O. (2024) Security and protection of information in electronic document management systems: Improving the level of cyber defense. *Bulletin of the Book Chamber*, 4, 39-44. doi: 10.36273/2076-9555.2024.4(333).39-44.

[11] Fetisov, O. (2024). Improving information security at enterprises through effective electronic document management systems (Edms). *Digital Economy and Economic Security*, 5(14), 153-159. doi: 10.32782/dees.14-24.

[12] Gani, D.H.A., Abd Kadir, I.K., Masrek, M.N., & Ab Rahman, A. (2024). An evaluation of electronic document management system functionalities and effectiveness in Malaysia. *European Proceedings of Social and Behavioural Sciences*, 133, 605-620. doi: 10.15405/epsbs.2024.05.50.

[13] González-Granadillo, G., González-Zarzosa, S., & Diaz, R. (2021). Security Information and Event Management (SIEM): Analysis, trends, and usage in critical infrastructures. *Sensors*, 21(14), article number 4759. doi:10.3390/s21144759.

[14] Han, J., & Son, Y. (2025). Design and implementation of a decentralized document management system. *Expert Systems with Applications*, 262, article number 125516. doi: 10.1016/j.eswa.2024.125516.

[15] Herrera Montano, I., García Aranda, J.J., Ramos Diaz, J., Molina Cardín, S., de la Torre Díez, I., & Rodrigues, J.J.P.C. (2022) Survey of techniques on data leakage protection and methods to address the insider threat. *Cluster Comput*, 25, 4289-4302. doi: 10.1007/s10586-022-03668-2.

[16] Jannah, R., Rizkyana, F.W., & Budiantoro, R.A. (2023). Audit of a web-based electronic documents and record management system (WEDRMS): Oversight efforts to improve administration in higher educational institutions. *BISECER (Business Economic Entrepreneurship)*, 5(2), 53-60. doi.org/10.61689/bisecer.v5i2.427.

[17] Kaur, K., Gupta, I., & Singh, A. (2017). A comparative evaluation of data leakage/loss prevention systems (DLPS). In *Conference: 3rd international conference on artificial intelligence and soft computing* (pp. 87-95). Zakopane: Springer. doi: 10.5121/csit.2017.71008.

[18] Kim, J., Park, M., Kim, H., Cho, S., & Kang, P. (2019). Insider threat detection based on user behavior modeling and anomaly detection algorithms. *Applied Sciences*, 9(19), article number 4018. doi: 10.3390/app9194018.

[19] Kondratyuk, S.S., & Palaguta, K.O. (2021). Choosing an electronic document management system: analysis of factors, current trends. *Computer Technologies for Data Processing*, 34-37.

[20] Koshara, A., & Bakalo, B. (2023). Improving the security of the public sector based on SIEM systems. *Infocommunication and Computer Technologies*, 2(04), 128-133. doi: 10.36994/2788-5518-2022-02-04-14.

[21] Kotwal, A.P. (2024). Leveraging Big Data analytics for enhanced cybersecurity: A comprehensive analysis of threat detection, incident response, and SIEM systems. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 10, 2158-2164. doi: 10.32628/CSEIT2410612414.

[22] Kovalska, L.A. (2021). Information and analytical activities in the work of the archive. *Information and Society*, 47-49.

[23] Landauer, M., Skopik, F., Stojanović, B., Flatscher, A., & Ullrich, T. (2025). A review of time-series analysis for cyber security analytics: From intrusion detection to attack prediction. *International Journal of Information Security*, 24, article number 3. doi: 10.1007/s10207-024-00921-0.

[24] Laue, T., Klecker, T., Kleiner, C., & Detken, K.-O. (2022). A SIEM architecture for advanced anomaly detection. *Open Journal of Big Data (OJBD)*, 6(1), 26-42. doi: 10.25968/opus-2321.

[25] Le, T.D., Le-Dinh, T., & Uwizeyemungu, S. (2025). Cybersecurity analytics for the enterprise environment: A systematic literature review. *Electronics,* 14(11), article number 2252. doi: 10.3390/electronics14112252.

[26] Levandovska, O.M. (2023) *Organizational and economic foundations of analytical support for enterprise activities*. (Doctoral dissertation, O.M. Beketov National University of Urban Economy in Kharkiv, Kharkiv, Ukraine).

[27] Liudvenko, D., Tomilova-Yaremchuk, N., Khomovyi, S., & Krupa N. (2023). Information security in the context of digitalization of document flow. *Scientific Collection "InterConf+"*, 33(155), 120-129. doi: 10.51582/interconf.19-20.05.2023.011.

[28] Martín, A.G., Beltrán, M., Fernández-Isabel, A., & Martín de Diego, I. (2021). An approach to detect user behaviour anomalies within identity federations. *Computers & Security*, 108, article number 102356. doi: 10.1016/j.cose.2021.102356.

[29] Muminova, S., Yuldasheva, N., & Safoev, N. (2022). Aspects of information security in the electronic document management system (EDMS) for bank system. *Research and Education*, 1(9), 331-340. doi: 10.5281/zenodo.7487114.

[30] Nazarova, I.Y. (2020). Possibilities and functions of electronic document management. *Economic Space*, 159, 166-170. doi: 10.32782/2224-6282/159-34.

[31] Noori, M., & Al-Hashimi, M. (2023). Evaluation of electronic document management systems: An overview. *Computer Integrated Manufacturing Systems*, 29(4), 273-294.

[32] Odintsov, O.M., Ilchenko, N.V., & Kryzhanivska, L.H. (2021). Introduction of electronic document technologies in public administration. *Collection of Scientific Papers of Cherkasy State Technological University. Series: Economic Sciences*, 60, 108-116. doi: 10.24025/2306-4420.1.60.2021.229175.

[33] Osazuwa, O.M.C. (2023). Confidentiality, integrity, and availability in network systems: A review of related literature. *International Journal of Innovative Science and Research Technology*, 8(12), 1946-1955. doi: 10.5281/zenodo.10464076.

[34] Paliy, S. (2022). Information and analytical activities in the development of information society. *Library Science. Record Studies. Informology*, 18(3), 76-80. doi: 10.32461/2409-9805.3.2022.266999.

[35] Perapu, P. (2025). Anomaly detection in user behaviour using machine learning for cloud platforms. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 11(3), 805-809. doi: 10.32628/CSEIT25113343.

[36] Politanskyi, V.S. (2021). Theoretical and legal basis of the electronic document management system in Ukraine. *Law and Society*, 1, 22-27. doi: 10.32842/2078-3736/2021.1.4.

[37] Saepulrohman, A., & Ismangil, A. (2021). Data integrity and security of digital signatures on electronic systems using the digital signature algorithm (DSA). *International Journal of Electronics and Communications Systems*, 1(1), 11-15. doi: 10.24042/ijecs.v1i1.7923.

[38] Savchuk, V., & Derii, V. (2023). Relevant analytics is a determining factor in effective management of the company's activities. *Herald of Economics*, 4, 104-117. doi: 10.35774/visnyk2023.04.104.

[39] Schwenk, J. (2022). Cryptography: Integrity and authenticity. In *Guide to internet cryptography. Information security and cryptography*. Cham: Springer. doi: 10.1007/978-3-031-19439-9_3.
[40] Shi, Y., Liu, Y., Tong, H., He, J., Yan, G., & Cao, N. (2020). Visual analytics of anomalous user behaviors: A survey. *IEEE Transactions on Big Data*, 8(2), 377-396. doi: 10.1109/TBDATA.2020.2964169.
[41] Sichkarenko, G., & Yaremko, S. (2022). Information and analytical support for professional activities: Concepts and functions. *Science and Technology Today*, 10(10), 303-314. doi: 10.52058/2786-6025-2022-10(10)-303-314.
[42] Somchenko, V., & Saienko, O., & Budko, D. (2024). Qualified electronic signature as a full-fledged legally valid signature for electronic document management and a tool for ensuring the security and authenticity of electronic documents and transactions. *Grail of Science*, 42, 112-119. doi: 10.36074/grail-of-science.02.08.2024.014.
[43] Splunk. (n.d.). Retrieved from https://www.splunk.com/en_us/products/enterprise-security.html.
[44] Sternad Zabukovšek, S., Jordan, S., & Bobek, S. (2023). Managing document management systems' life cycle in relation to an organization's maturity for digital transformation. *Sustainability*, 15(21), article number 15212. doi: 10.3390/su152115212.
[45] System of electronic interaction of executive authorities (SEI EA). (n.d.). Retrieved from https://se.diia.gov.ua/en/sev-ovv?utm_source.
[46] Tekin, S., Bicakci, K., Mersin, O., Erdem, G.N., Canbay, A., & Uzunay, Y. (2023). Optimal data backup policies for information systems subject to sudden failure. *Journal of Quality in Maintenance Engineering*, 29(2), 338-355. doi: 10.1108/JQME-01-2022-0009.
[47] Tkachenko, O., & Humeniuk, M. (2020). Some aspects of statistical and scientific data visualization. *Digital Platform: Information Technologies in Sociocultural Sphere*, 3(2), 134-147. doi: 10.31866/2617-796x.3.2.2020.220584.
[48] Vchasno group. (n.d.). *We create innovative products for Ukrainian entrepreneurs*. Retrieved from https://vchasno.group/.
[49] Vchasno. (n.d.). *Electronic document management in Ukraine*. Retrieved from https://vchasno.ua/?utm.
[50] Voronkova, V., Koshelevsky, V., & Lisitsa, S. (2024). Digital transformation of information and analytical support of management processes in modern organizations in the context of global digitalization. *Digital Economy and Economic Security*, 5(14), 33-41. doi: 10.32782/dees.14-5.
[51] Walters, A. (2025). *What is an electronic document management system (EDMS)?* Retrieved from https://www.irisglobal.com/blog/what-is-an-electronic-document-management-system/?utm_source.
[52] What is an audit trail in document management? (n.d.). Retrieved from https://www.folderit.com/glossary/what-is-an-audit-trail-in-document-management/?utm_source.
[53] Yasinska, A. (2022). Problems and prospects of electronic document management in the context of digital transformation. *Young Scientist*, 11(111), 128-134. doi: 10.32839/2304-5809/2022-11-111-27.
[54] Zahumenna, V., & Kuzmenko, O. (2022). Information and analytical activity as a scientific and educational discipline: Evolution, development trends. *Library Science. Record Studies. Informology*, 18(4), 102-107. doi: 10.32461/2409-9805.4.2022.269817.
[55] Zhou, J., & Zhang, W. (2024). AI in archival science – a systematic review. *arXiv*. doi: 10.48550/arXiv.2410.09086.
[56] Zozulya, N., Stekolshchikova, V., & Shoturma, N. (2025). Information and analytical activities in the age of digital transformation: New tools and methodologies. *Scientific Works of the Interregional Academy of Personnel Management. Philology*, 1(15), 21-26. doi: 10.32689/maup.philol.2025.1.4.

# Інформаційно-аналітична діяльність як фактор підвищення інформаційної безпеки та достовірності даних в системах електронного документообігу

**Оксана Плужник**
Доктор філософії, доцент
Університет Григорія Сковороди в Переяславі
08401, вул. Сухомлинського, 30, м. Переяслав, Україна
https://orcid.org/0000-0001-8780-8288
**Владислав Дуда**
Викладач
Університет Григорія Сковороди в Переяславі
08401, вул. Сухомлинського, 30, м. Переяслав, Україна
https://orcid.org/0009-0001-0048-4805

**Анотація.** Актуальність дослідження зумовлена зростаючою потребою у використанні інформаційно-аналітичної діяльності (ІАД) як ключового інструмента забезпечення інформаційної безпеки та достовірності даних в умовах активного впровадження систем електронного документообігу (СЕДО) у цифровізованому суспільстві. Метою дослідження було комплексне розкриття ролі інформаційно-аналітичної діяльності (ІАД) у підвищенні рівня інформаційної безпеки та забезпеченні достовірності даних в системах електронного документообігу. У процесі дослідження застосовано методи системного аналізу, огляду наукових джерел та синтезу інформації, а також критичний аналіз сучасних технічних засобів. Результати дослідження підтвердили, що ІАД є критично важливим чинником для забезпечення захисту інформаційних ресурсів і збереження достовірності даних у СЕДО. Комплексні можливості збору, обробки, аналізу та інтерпретації інформації забезпечують своєчасне виявлення загроз, ефективне прогнозування ризиків, контроль за повним життєвим циклом документів та верифікацію їх автентичності. Це дозволяє не лише оперативно реагувати на інциденти, але й формувати дієві політики безпеки, що знижують ймовірність втрат, спотворення або несанкціонованого доступу до даних. Виявлено ключові виклики, серед яких – брак висококваліфікованих фахівців із міждисциплінарними компетенціями, складнощі інтеграції різнорідних систем та правові й етичні обмеження, пов'язані із захистом персональних даних та прозорістю алгоритмів аналізу. Перспективи розвитку ІАД і СЕДО пов'язані з активною інтеграцією технологій штучного інтелекту та машинного навчання для автоматизованого виявлення аномалій і прогнозування загроз, застосуванням блокчейн-рішень для забезпечення незмінності даних та використанням інструментів Big Data для виявлення прихованих закономірностей. Подолання зазначених викликів і впровадження інноваційних підходів сприятиме зміцненню надійності, безпеки та довіри до цифрових документів. Практичне значення дослідження полягає в можливості використання результатів для підвищення ефективності функціонування систем електронного документообігу за рахунок інтеграції інформаційно-аналітичних інструментів, спрямованих на забезпечення інформаційної безпеки та достовірності даних

**Ключові слова:** аналітичні системи; системи моніторингу; аналітика подій безпеки; безпека інформаційних систем; цифрова трансформація; SIEM системи