4. Oleinik S. V. & Stykhar I. Ya. (2015*). Fond ridkisnykh vydan yak vazhlyvyi faktor zabezpechennia naukovo-doslidnoidiialnosti u vyshchomu navchalnomu zakladi (na prykladi naukovoi biblioteky prykarpatskoho natsionalnoho universytetu imeni Vasylia Stefanyka).* Ivano-Frankivsk: Vyd-vo NB DVNZ, pp. 206—213.
14. Pravyla korystuvannia naukovo-tekhnichnoiu bibliotekoiu Natsionalnoho aerokosmichnoho universytetu im. M. Ye. Zhukovskoho "KhAI" (n. d.). *Natsionalnyi aerokosmichnyi universytet im. M. Ye. Zhukovskoho "KhAI" : vebsait.* Available at: https://library.khai.edu/pravila-koristuvannya-naukovo-tehnyachnoyu-byablyaotekoyu-nacyaonalnogo-aerokosmyachnogo-unyaversitetu-yam.-m.-ya.-zhukovskogo-haya.
5. Pravyla korystuvannia Naukovo-tekhnichnoiu bibliotekoiu Natsionalnoho aviatsiinoho universytetu. *Naukovo-tekhnichna biblioteka Natsionalnoho aviatsiinoho universytetu : vebsait*. Available at: http://www.lib.nau.edu.ua /about/RulesNew.htm.
6. Pro biblioteku (n. d.). *Natsionalnyi aerokosmichnyi universytet im. M. Ye. Zhukovskoho "KhAI" : vebsait.* Available at: https://library.khai.edu/pro-byablyaoteku.
7. Pro biblioteku (n. d.). *Naukovo-tekhnichna biblioteka Natsionalnoho aviatsiinoho universytetu : vebsait* Available at: http://www.lib.nau.edu.ua/about/.
8. Fondy ta kolektsii (n. d.). *NTB Natsionalnoho tekhnichnoho universytetu Ukrainy "Kyivskyi politekhnichnyi instytut imeni Ihoria Sikorskoho" : vebsait.* Available at: https://www.library.kpi.ua/resources/fondy-ta-kolektsiyi/#special _collections.
9. Kharytonenko O. (2019). "Represovani" ta "reabilitovani" pidruchnyky z kolektsii Naukovoi biblioteky NPU im. M. P. Drahomanova. *Visnyk Knyzhkovoi palaty*, 8, pp. 48—52.
10. Tsyfrova biblioteka (n. d.). *NTB Natsionalnoho tekhnichnoho universytetu Ukrainy "Kyivskyi politekhnichnyi instytut imeni Ihoria Sikorskoho" : vebsait*. Available at: https://dil.kpi.ua/dlibra.
11. Tsinni vydannia kintsia XIX — pochatku XX st. Z fondu Naukovo-tekhnichnoi biblioteky Natsionalnoho aviatsiinoho universytetu. Ch. 1. Aviatsiia. Povitroplavannia (1897—1940): *retrospektyvnyi bibliohrafichnyi pokazhchyk* (2018). Kyiv: NAU.
12. Chasti zapytannia (n. d.). *NTB Natsionalnoho tekhnichnoho universytetu Ukrainy "Kyivskyi politekhnichnyi instytut imeni Ihoria Sikorskoho" : vebsai*t. Available at: https://www.library.kpi.ua/faq/.

Надійшла до редакції 15 лютого 2024 року

ІНФОРМАЦІЙНА ДІЯЛЬНІСТЬ

УДК 005.922-028.27:004.056](477)(045)
DOI: 10.36273/2076-9555.2024.4(333).39-44

Olesia Fedoruk,
Doctor of Philosophy (PhD),
Senior Teacher of the Department of Document Studies
and Information Activitiesof the National University of Ostroh Academy,
e-mail: olesia.fedoruk@oa.edu.ua
ORCID: https://orcid.org/0000-0001-7646-9604

Security and protection of information in electronic document management systems: improving the level of cyber defense

The article describes the main threats to electronic document management systems. The importance of the electronic document management system for organizational processes of enterprises and information security is considered. Particular importance is the use of electronic document management systems for the efficiency and speed of performing organizational functions.

The article analyzes the aspects of information security when using electronic document management systems in practice and the effectiveness of implementation to ensure information security in comparison with traditional paper document management. The importance of the Information Security Strategy until 2025, approved by the Cabinet of Ministers of Ukraine, is emphasized. Attention is focused on the advantages of using the stages of implementing the cybersecurity model in electronic document management systems to protect information and data.

It also discusses best practices for secure document storage and sharing that promote an integrated approach to various aspects of document management security to protect confidential information from potential cyber threats. The criteria for choosing a high-quality electronic document management system, for ensuring information security and countering cyber attacks are quite important.

In particular, attention is focused on modern antivirus technologies that allow detecting almost all known viruses by comparing the code of a suspicious file with samples stored in the antivirus database. Therefore, for organizations seeking to use the latest technologies, information security is essential in electronic document management systems to increase the level of cybersecurity.

Keywords: *information security; electronic document management systems; threats; cybersecurity; documents*

The problem in general. Modern society is transforming into an era of digitalization of management processes, replacing paper-based workflow with electronic one. Accordingly, the problem of information security arises, since the basic element of any electronic document management system is a document.

There is a need to protect not only documents, but also the operability of electronic document management systems, ensuring quick recovery from damage, failures or cyberattacks. The protection of electronic document management systems should be comprehensive and provide for protection at all levels, from the protection of physical media and data to organizational measures.

The main problem today is the effective protection of information, namely the protection of documents and the preservation of information from unauthorized access.

Therefore, today there is a problem of comprehensive protection of electronic systems. In particular, it is necessary to protect the hardware elements of the system, it is necessary to provide for the protection of the system files of the software and database, and documents and information stored within the system should also be protected.

Analysis of researches and publication. Today, there is a problem of full-fledged information security in electronic document management systems. Most modern organizations are not equipped with the proper tools to implement effective protection of electronic document management systems, which leads to system failures, document destruction and cybercriminals taking possession of sensitive information.

For the study of this problem, works on information security and cybersecurity in the activities of organizations are of particular importance (I. Sopilko [11], O. Panchenko [9], N. Kukharska [3], O. Polotai [3], A. Azarova [1], I. Dohtieva, A. Shyian, and others); legal support of information security (Y. Kuniev, V. Vyzdryk, O. Melnyk); information security in electronic document management systems (L. Piddubna [10], V. Pavlichenko).

The literature analysis shows that the topic is relevant to today's realities. At the same time, the topic is not sufficiently researched, as many aspects remain open.

The purpose of the article is to substantiate information security in electronic document management systems and to overcome the main threats of cyber attacks.

Presentation of main materials. Today, organizations are actively implementing electronic document management systems to implement management processes. The popularization of electronic document management systems is driven by the digitalization of production processes and the efficiency of using electronic documents. At the same time, if we compare the protection of paper and electronic documents, it is usually impossible to protect paper versions of documents with several levels of protection as it is possible with electronic forms of documents.

In today's organizational environment, information is one of the most valuable assets. Today, cybercrime is becoming more sophisticated, and information security has become a critical need. The electronic world penetrates all the constituent elements of the organizational processes of enterprises, and today there are many threats to electronic document management systems. Today, one of the most important requirements for any electronic document management system is to ensure information security of electronic document exchange. According to the Law of Ukraine "On Protection of Information in Information and Telecommunication Systems" [8], information protection is an activity aimed at preventing unauthorized actions with respect to information in the system. At the same time, the responsibility for ensuring the protection of information lies with the system owner.

In accordance with the current realities of global information security, the main threats to electronic document management systems can be classified as follows:

— threat to integrity — is the damage, destruction or distortion of information, which can be either unintentional in cases of errors and failures or malicious;

— threat to confidentiality — is any violation of confidentiality, including theft, interception of information, change of routes, etc.;

— threat to system performance — is a threat, the realization of which leads to disruption or termination of the system, including intentional attacks, user errors, as well as hardware and software failures;

— impossibility to prove authorship — this is a threat that is expressed in the fact that if an electronic digital signature is not used in the document flow, it is impossible to prove that it was this user who created the document (and it is impossible to make the document flow legally significant);

— threat to availability — is a threat that disrupts the ability of users who have the right to access it to obtain the necessary information within a reasonable time [5].

Information stored on servers is usually protected by access control and encryption. If the entire corporate network of an organization is located within a single local computer system, this may be sufficient to protect confidential information. However, if the organization has an extensive structure, including branches, structural units, regional offices and employees working in remote locations, the issue of information security when exchanging confidential data becomes more important [14].

In real working conditions, information security can be violated due to many factors, namely: unauthorized dissemination of information, use and violation of the integrity, confidentiality and availability of information; negative information influence; fraud in trade and financial transactions; unauthorized access to organizational management systems, technological processes and cyber attacks.

Today, any organization should understand that the most important function of any electronic document management system is to ensure information security and electronic document exchange, so when implementing electronic document management systems in the activities of organizations, it is necessary to protect electronic document flow. This is due to the increase in the number of confidential documents in public authorities and organizations of various forms of ownership and the active transition to electronic document management systems. The approach to protecting electronic document management should be comprehensive. It is necessary to clearly assess the possible threats and risks of electronic document management systems and the possible losses from realized threats [5].

Particular importance is the use of electronic document management systems for the efficiency and speed of performing organizational functions. Information security aspects are predominant in the presence or absence of electronic document management systems in an organization, which is why the use of electronic document management systems in practice is more effective in ensuring information security than traditional paper-based document management (table 1).

Table 1

Comparative aspects of information security of paper document flow and electronic document flow

Information security aspect	Using traditional paper-based workflow	Using an electronic document management system
Unauthorized access	Physical documents can be stolen or viewed by unauthorized persons	Access to digital documents is limited and can be controlled by security measures such as passwords and encryption
Data backup	Lack of appropriate backups can lead to permanent loss of documents in the event of a disaster, fire or physical damage	Digital documents can be backed up regularly and stored securely in multiple locations, minimizing the risk of loss
Control and audit	It is difficult to track who had access to physical documents and what changes were made	Electronic document management systems can record and verify every access and modification, providing control over the history of changes
Compliance with regulatory requirements	Compliance can be difficult without a system that ensures document control and security	Electronic document management systems often include special functions for compliance with legal regulations, which simplifies the process
Secure cooperation	Collaborating on physical documents can be risky, as documents can be lost or shared with unauthorized people	Collaboration on electronic documents is secure and controlled, reducing the risk of information leakage

Source: by the author

Cyberwarfare and cyberterrorism are becoming global in nature and have a pronounced dynamic, which complicates their detection and counteraction. The number of unauthorized interference with computers that does not meet the standards of the International Convention on Cyber Security has also increased [2].

In particular, on September 15, 2021, the Cabinet of Ministers of Ukraine approved the Information Security Strategy until 2025 [13]. The strategy envisages countering internal and external threats to information security, protecting the state sovereignty and territorial integrity of Ukraine, supporting social and political stability, state defense, and ensuring the rights and freedoms of every citizen through information means and measures.

The results of the Strategy implementation should include:

— secure information space;

— effective functioning of the strategic communications system;

— effective counteraction to the spread of illegal content;

— information reintegration of Ukrainian citizens living in the temporarily occupied territories and adjacent territories of Ukraine;

— increasing the level of media culture and media literacy of the population;

— ensuring the protection of journalists' rights;

— formation of a national identity [7].

It should be emphasized that as document management continues its long transition from physical documents to digital databases and cloud storage, the potential for cyber threats is growing every year. As such, it is critical that organizations understand and address the link between document management and cybersecurity. In this case, information security remains a broader area and is applied to document management, and cybersecurity is aimed at digitizing documents [6].

Particular importance is the use of the stages of implementing the cybersecurity model in electronic document management systems to protect information and data:

1. Professional management of information and documents, granting access rights only to competent and responsible employees.

2. Use of data classification technologies and risk-based information for organizational processes.

3. Implementation of security criteria for access to cloud storage and implementation of data leakage prevention technologies. Use of technologies that block abnormal connections.

4. Effective protection of data and information — providing controls that restrict access to specific documents based on content, appointing responsible persons for information protection.

Secure document storage and sharing best practices can be grouped into categories that promote a holistic approach to various aspects of document management security to protect sensitive information from potential cyber threats, including:

— data classification and security measures, including the practice of classifying documents based on confidentiality, encrypting stored documents and data in transit, implementing strict access controls, and using multi-factor authentication to access documents;

— collaboration and user training ensures practices such as the use of secure collaboration platforms, as well as training employees in cybersecurity and best practices for document management;

— monitoring and response methods include continuous monitoring of access to documents and changes in the content of documents, as well as the development of a clearly defined incident response plan;

— the control policy provides for the establishment of clear stages of storage, destruction and ensures that document management is in line with industry standards;

— backup and data security practices are related to regular backup of documents and selection of reputable cloud providers with strict data security policies;

— software management and vendor consultation includes keeping software and tools up-to-date and meeting security standards;

— ontinuity of organizational processes and secure document sharing include practices such as developing a contingency plan, using secure file transfer methods when sharing documents, and blocking access for employees who leave.

The main criteria for choosing a high-quality electronic document management system to ensure information security and counteract cyber attacks: ensuring the safety of electronic documents; closed access to the electronic document management system; delimitation of access rights; observance of the degree of confidentiality in electronic document management systems; cryptographic methods of data encryption may be used; ensuring the reliability of information; logging of actions of users of electronic document management systems. If properly configured and implemented, logging in electronic document management systems makes it possible to track all illegal actions of users, and in case of prompt intervention, even stop an attempt of illegal or harmful actions [4].

The concept of information security is not limited to the security of technical information systems or the security of information in numerical or electronic form, but concerns all aspects of data or information protection regardless of the form in which it is stored. Therefore, information security is the state of the level of security of the information environment, and information protection is an activity aimed at preventing leakage of protected information from unintentional and unauthorized influences on the protected information, i.e. a process aimed at achieving this state [4].

A much more effective solution for protecting an electronic document is to assign security parameters that are an integral part of the document itself, such parameters include criteria that determine the permanent security of the document: Confidentiality, Authorization, Accountability, Integrity, Authenticity, Non-repudiation (fig. 1).

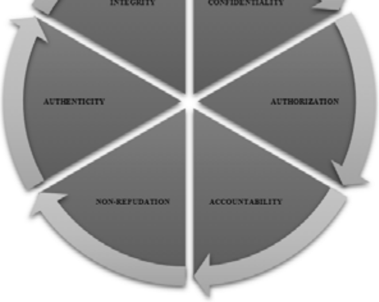

Fig. 1. Six key criteria for keeping documents secure at all time

Source: [12, p. 334]

Each of these methods can be used both independently and in integration with others. Modern antivirus technologies can detect almost all known viruses by comparing the code of a suspicious file with samples stored in the antivirus database. In addition, behavioral modeling technologies have been developed to detect newly created virus programs [12, p. 337].

Conclusions. In the digital era information security should be a priority for all organizations seeking to protect sensitive data. Any electronic document management system must provide protection against threats, because organizing and implementing information for management needs increases the risk of threats.

The protection of electronic document management systems must be comprehensive at all levels, from the protection of physical media and data to organizational measures.

Thus, protecting information and increasing cyber security is one of the main areas of improving the efficiency, accuracy and quality of management functions and interaction between organizations. Therefore, the current perspective of organizations is a vector for electronic document management with the use of information and data protection functions.

References

1. Azarova A. O., Dohtieva I. O. & Shyian A. A. (2022). Decision support system for improving the level of information security of the enterprise. *Information technology and computer engineering,* 1, pp. 12—18.
2. Information security now: what elements are missing? Available at: https://ecpl.com.ua/news/informatsiyna-bezpeka-now-iakykh-elementiv-ne-vystachaie.
3. Kukharska N. P. & Polotai O. I. (2019). Aspects of information security in the management of the continuity of the organization. *Collection "Information Technology and Security"*, issue 7, № 2 (13), pp. 26—136.
4. Kunev Y. D. (2021). Legal support of information security as a subject of legal research. *Legal Bulletin "Air and Space Law"*, 1 (58), pp. 95—1026.
5. Maznychenko N. I. (2014). Information protection in electronic document management systems based on identification systems. *Computer modeling in science-intensive technologies.* International scientific and technical conference (May 28—31, 2014, Kharkiv). Kharkiv, pp. 1—2.
6. *On the Basic Principles of Ensuring Cybersecurity of Ukraine* : Law of Ukraine at 5.X.2017 N 2163-VIII. Available at: https://zakon.rada.gov.ua/laws/show/2163-19#Text.
7. *On the decision of the National Security and Defense Council of Ukraine of May 14, 2021 "On the Cybersecurity Strategy of Ukraine"* : Decree of the President of Ukraine of 26.08.2021 No. 447/2021. Available at: https://www.president.gov.ua/documents/4472021-40013.
8. *On the Protection of Information in Information and Communication Systems* : Law of Ukraine at 5.07.1994 N 80/94-ВР. Available at: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.
9. Panchenko O. A. (2020). Information security in the context of challenges and threats to national security. *Public Administration and Local Self-Government,* 2, pp. 57—63.
10. Piddubna L. V. & Pavlichenko V. M. (2019). Information security in electronic document management systems. *Scientific Bulletin of PUET. Series "Economic Sciences"*, 4 (95), pp. 59—66.
11. Sopilko I. M. (2021). Information security and cybersecurity: comparative legal aspect. *Legal Bulletin of Air and Space Law*, 2 (59), pp. 110—115.
12. 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), pp. 331—340. Available at: https://doi.org/10.5281/zenodo.7487114.
13. *The Government approved the Information Security Strategy until 2025.* Available at: https://www.kmu.gov.ua/news/uryad-shvaliv-strategiyu-informacijnoyi-bezpeki-do-2025-roku.
14. Vyzdryk V. S. & Melnyk O. M. (2023). Information security in Ukraine: current state. *Grail of Science*, 24, pp. 196—202.

Олеся Федорук,
докторка філософії (PhD),
старша викладачка кафедри
інформаційно-документних комунікацій
Національного університету "Острозька академія"

Безпека та захист інформації у системах електронного документообігу: підвищення рівня кіберзахисту

У статті подано опис основних загроз для систем електронного документообігу. Розглянуто важливість системи електронного документообігу для організаційних процесів підприємств та забезпечення інформаційної безпеки. Особливе значення має використання систем електронного документообігу для ефективності та швидкості виконання організаційних функцій.

Проаналізовано аспекти інформаційної безпеки у процесі практичного використання систем електронного документообігу та ефективність реалізації в порівнянні з традиційним паперовим документообігом. Наголошено на важливості схваленої Кабінетом Міністрів України Стратегії інформаційної безпеки до 2025 р. Акцентовано на перевагах у використанні етапів впровадження моделі кібербезпеки в системи електронного документообігу для захисту інформації та даних.

Розглянуто оптимальні методи безпечного зберігання та обміну документами, які сприяють комплексному підходу до різних аспектів безпеки керування документами для захисту конфіденційної інформації від потенційних кіберзагроз. Підсумовано, що важливими є критерії для вибору якісної системи електронного документообігу, для забезпечення інформаційної безпеки та протидії кібератакам.

Зосереджено увагу на сучасних антивірусних технологіях, що дають змогу виявити майже всі відомі вірусні програми через порівняння коду підозрілого файлу зі зразками, що зберігаються в антивірусній базі. Підсумовано, що для організацій, які прагнуть використовувати новітні технології, захист інформації є вагомим та обов'язковим складником у системах електронного документообігу для підвищення рівня кіберзахисту.

Ключові слова: *захист інформації; системи електронного документообігу; загрози; кіберзахист; документи*

Список бібліографічних посилань

1. Азарова А. О, Дьогтєва І. О, Шиян А. А Система підтримки прийняття рішень щодо підвищення рівня інформаційної безпеки підприємства. *Інформаційні технології та комп'ютерна інженерія*. 2022. № 1. С. 12—18.
2. Інформаційна безпека now: яких елементів не вистачає? URL: https://ecpl.com.ua/news/informatsiyna-bezpeka-now-iakykh-elementiv-ne-vystachaie/.
3. Кухарська Н. П., Полотай О. І. Аспекти інформаційної безпеки в управлінні безперервністю діяльності організації. *Збірник "Information Technology and Security*". 2019. Вип. 7. № 2 (13). С. 126—136. URL: https://sci.ldubgd.edu.ua/jspui/handle/123456789/7172.
4. Кунєв Ю. Д. Правове забезпечення інформаційної безпеки як предмет правового дослідження. *Юридичний вісник "Повітряне і космічне право"*. 2021. № 1 (58). С. 95—102. URL: https://dspace.nau.edu.ua/bitstream/NAU/53719/1/%d0%ae.%20%d0%94.%20%d0%9a%d1%83%d0%bd%d1%94%d0%b2.pdf.
5. Мазниченко Н. І. Захист інформації в системах електронного документообігу на основі систем ідентифікації. *Комп'ютерне моделювання в наукомістких технологіях*. Міжнар. наук.-техн. конф. (28—31 трав. 2014 р., Харків). Харків, 2014. С. 1—2. https://dspace.nlu.edu.ua/bitstream/123456789/6710/1/Maznichenko.pdf.
6. Про основні засади забезпечення кібербезпеки України : Закон України від 5.X.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.
7. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України" : Указ Президента України від 26.08.2021 № 447/2021. URL: https://www.president.gov.ua/documents/4472021-40013.
8. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 5.07.1994 № 80/94- ВР. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.
9. Панченко О. А. Інформаційна безпека в контексті викликів і загроз національній безпеці. *Публічне управління та місцеве самоврядування*. 2020. № 2. С. 57—63.
10. Піддубна Л. В., Павліченко В. М. Інформаційна безпека в системах електронного документообігу. *Науковий вісник ПУЕТ*. Серія "Економічні науки". 2019. № 4 (95). С. 59—66.
11. Сопілко І. М. Інформаційна безпека та кібербезпека: порівняльно-правовий аспект. *Юридичний вісник Повітряне і космічне право*. 2021. № 2 (59). С. 110—115.
12. Muminova S., Yuldasheva N., Safoev N. Aspects of Information Security in the Electronic Document Management System (EDMS) for Bank System. *Research and Education*. 2022. № 1 (9), 331—340. URL: https://doi.org/10.5281/zenodo.7487114 https://zenodo.org/records/7487114.
13. Уряд схвалив Стратегію інформаційної безпеки до 2025 року. URL: https://www.kmu.gov.ua/news/uryad-shvaliv-strategiyu-informacijnoyi-bezpeki-do-2025-roku.
14. Виздрик В. С., Мельник О. М. Інформаційна безпека в Україні: сучасний стан. *Grail of Science*. 2023. № 24. С 196—202. doi: https://doi.org/10.36074/grail-of-science.17.02.2023.034.

Надійшла до редакції 21 березня 2024 року