



ORIGINAL

Regulatory framework for e-documentation and cyber protection amidst society's digital shift

Marco normativo para la documentación electrónica y la ciberprotección en medio del cambio digital de la sociedad

Valentina Petrovich¹  , Lidiia Moskvych² , Nataliia Shcherbakova³ , Lina Doroshenko⁴ , Oleksandr Aloslyn⁵ 

¹Lesya Ukrainka Volyn National University, Department of Museology, Monument Studies and Information and Analytical Activities. Lutsk, Ukraine.

²Yaroslav Mudryi National Law University, Faculty of Prosecutor's Office, Department of Criminal Procedure. Kharkiv, Ukraine.

³Vasyl' Stus Donetsk National University, Law Faculty, Department of Civil Law and Process. Vinnytsia, Ukraine.

⁴Vasyl' Stus Donetsk National University, Law Faculty, Department of Economic and Administrative Law. Vinnytsia, Ukraine.

⁵Interregional Academy of Personnel Management. Kyiv, Ukraine.

Cite as: Petrovich V, Moskvych L, Shcherbakova N, Doroshenko L, Aloslyn O. Regulatory framework for e-documentation and cyber protection amidst society's digital shift. Salud, Ciencia y Tecnología - Serie de Conferencias. 2025; 4:1336. <https://doi.org/10.56294/sctconf20251336>


Submitted: 21-05-2024

Revised: 24-08-2024

Accepted: 02-12-2024

Published: 01-01-2025

Editor: Prof. Dr. William Castillo-González 

Corresponding author: Valentina Petrovich 

ABSTRACT

Introduction: Ukraine's active integration into the European community emphasises the crucial role of digital technologies in ensuring the population's welfare and the country's economic growth. Studying the peculiarities of electronic document management in the EU countries will help avoid mistakes and develop an effective system that will meet European standards in many countries on the way to Europeanisation.

Objectives: analyse the legal aspects of electronic document management, identify security issues in the information space in Ukraine, and assess Ukrainian e-justice compliance with European standards in the context of digital transformation.

Method: it was conducted using general scientific methods, including analysis of legal documents, generalisation, synthesis, system analysis, analytical diagnostics, and statistical data analysis.

Results: it is proved that the legal support of the electronic document management system ensures centralised management of documents, their entire life cycle, collaboration, confidentiality, automatic routing and integration with other systems by the legal documents establishing the legal framework on which the relations between the participants to the process are built, defining their rights, duties and responsibilities.

Conclusion: the article identifies the main areas of development and problematic aspects of implementing the e-justice system at the current stage of its formation, as well as the prospects for introducing new technologies in this area.

Keywords: Digital Transformation; Information And Communication Technologies; Cybersecurity; Legal Support; Electronic Document Management, E-Government.

RESUMEN

Introducción: la integración activa de Ucrania en la comunidad europea pone de relieve el papel crucial de las tecnologías digitales para garantizar el bienestar de la población y el crecimiento económico del país. Estudiar las peculiaridades de la gestión electrónica de documentos en los países de la UE ayudará a evitar

errores y a desarrollar un sistema eficaz que cumpla las normas europeas en muchos países en vías de europeización.

Objetivos: analizar los aspectos legales de la gestión electrónica de documentos, identificar los problemas de seguridad en el espacio de la información en Ucrania y evaluar la conformidad de la justicia electrónica ucraniana con los estándares europeos en el contexto de la transformación digital.

Método: se llevó a cabo utilizando métodos científicos generales, incluyendo análisis de documentos legales, generalización, síntesis, análisis de sistemas, diagnósticos analíticos y análisis de datos estadísticos.

Resultados: se demuestra que el soporte legal del sistema de gestión electrónica de documentos garantiza la gestión centralizada de los documentos, todo su ciclo de vida, la colaboración, la confidencialidad, el enrutamiento automático y la integración con otros sistemas mediante los documentos legales que establecen el marco jurídico sobre el que se construyen las relaciones entre los participantes en el proceso, definiendo sus derechos, deberes y responsabilidades.

Conclusiones: el artículo identifica las principales áreas de desarrollo y los aspectos problemáticos de la implementación del sistema de e-justicia en la fase actual de su formación, así como las perspectivas de introducción de nuevas tecnologías en este ámbito.

Palabras clave: Transformación Digital; Tecnologías de La Información y la Comunicación; Ciberseguridad; Apoyo Jurídico; Gestión Electrónica de Documentos; Administración Electrónica.

INTRODUCTION

The deep penetration of digital technologies in all spheres of social life has created a new reality characterised by dynamic development, modernisation and transformation of all aspects of human activity, from the economy to public administration. Intelligent digital technologies such as artificial intelligence, machine learning and big data are revolutionising how people work, do business, learn and interact. Rapid changes in remote interaction driven by the development of digital technologies make it necessary to constantly update the legal framework to ensure effective management of social relations in the digital environment. Creating a favourable environment for the development of digital technologies is impossible without constantly updating legislation that must meet the challenges of the modern digital age. The definition of specific tasks within digital transformation programmes requires a comprehensive analysis of national characteristics, including cultural context, level of socio-economic development and availability of financial resources.

The document flow in government agencies is challenging to automate due to its multifunctionality. It includes the registration, processing, storage and use of large documents, which is critical for effective management and provision of services to citizens. One of the most pressing issues today is to empower citizens to influence state-building processes with the help of modern information and communication technologies, in particular, introducing an electronic document management system as a high-tech tool for interaction, which requires the development of a clear legal framework. The European Union has achieved significant success in developing electronic document management; thanks to a clear legislative framework and advanced technologies, electronic documents have become essential to business processes and interaction with government bodies.

The ongoing process of developing electronic democracy and a knowledge society also requires constant modernisation in this area, as legal provisions concerning electronic document circulation must be adapted to new global realities.

Electronic justice is also a powerful mechanism for the consolidation of the rule of law and adequate protection of human rights. Simply put, it enables streamlining the procedures, enhances court process transparency, and serves towards effective justice for all. Technology is, by all means, beneficial and a projected pillar of assistance offered to us in relation to the construct that is society; they are also dangerous due to their use for not-so-well-intentioned behaviour, i.e., manipulation and crime. Thus, the implementation of electronic justice in human rights and rule-of-law jurisdiction should aim at understanding what it can do well while minimising potential harm.

Literature review

Previous research on digital transformation and technology adoption throughout economies comes from almost 20 years ago and established a strong global policy response. The impact of digital changes on society has been researched actively over the last several decades. Researchers such as Boulton⁽¹⁾, Buhrimenko and Smirnova⁽²⁾ have considered economic, political sociocultural transformations based on global technologies like AI, Internet Things BigData Digital transformation is more than a reshuffling of the proverbial deck: it's an implied rearrangement and top-down restructuring of business models, consumer behaviour patterns, and even national social relationships.⁽³⁾

Scientific research covers various aspects of digital changes in society; in particular, Pawełoszek *et al.*⁽⁴⁾ in their works justify the need for the integrated use of blockchain, artificial intelligence, and the Internet of Things to ensure effective digital transformation of organisations and assess the legitimacy of their application. Thanks to the progress of technology and the constant development of the digital space, organisations can effectively manage their resources, optimise business processes, and, as a result, achieve significant competitive advantages.⁽⁵⁾

Despite the apparent advantages of digital transformation, it also raises several problems related to data security, the spread of disinformation and the risks of social exclusion caused by excessive dependence on digital technologies, as emphasised by Khaustova.⁽⁶⁾ The spread of digital technologies in all spheres of public life is accompanied by the emergence of new types of cyber threats, which require constant adaptation to new legal norms and information security technologies. Bondarenko *et al.*⁽⁷⁾ emphasise that they provide for further detailing and clarification of existing legal norms, development of new standards and procedures in the field of information security, as well as strengthening of state control over their implementation. Nurahman⁽⁸⁾, Ismanto *et al.*⁽⁹⁾, Siregar and Sinaga⁽¹⁰⁾, Putri *et al.*⁽¹¹⁾, Syahril⁽¹²⁾, in their scientific work prove that legislation, in particular, Ukrainian, does not keep pace with the rapid pace of development of cybercrime, which leads to ineffective combating of this phenomenon. Despite the desire for European integration and compliance with European cybersecurity standards, Ukrainian legislation still lacks universal tools to effectively combat cybercrime, especially that committed by state authorities.^(13,14)

The development of information technology has led to the fact that electronic documents have become the primary carrier of information processed and transmitted by ICT, as noted by Kiu *et al.*⁽¹⁵⁾. The electronic document management system is constantly evolving due to the development of new technologies such as artificial intelligence and blockchain, opening up new opportunities for automating business processes and improving work efficiency, according to Benmakhlouf and Chouaou.⁽¹⁶⁾

As an integral part of e-governance, e-courts make the judicial system more transparent and accessible to citizens by ensuring that court procedures are open and accessible.⁽¹⁷⁾ Orioque *et al.*⁽¹⁸⁾ prove that an online document management system is the optimal solution for quick and convenient access to the necessary documents when dealing with legal issues. Automation of the processes of submitting documents, their consideration and decision-making significantly increases the efficiency of case consideration, the ability to submit documents electronically, track the progress of a case online, participate in court hearings remotely, public access to information on the progress of a case, all contribute to increasing trust in the judicial system as a whole, which is an urgent issue today, according to Bouchoux.⁽¹⁹⁾

The widespread introduction of e-justice will significantly improve the quality of justice delivery and increase the efficiency of all structures of the judicial system. Given the constant development of new technologies, introducing electronic document management in the judicial system requires adaptation of legal norms, new regulatory mechanisms, and additional research.

The work aims to study the current state of legal support for electronic document management and substantiate the problems of information space security in the context of society's digital transformation in e-government, particularly in e-justice. The author's task is to substantiate the current state and trends of e-justice development by European standards.

METHOD

The study used general scientific methods, including generalisation, synthesis, specific historical, systemic, logical and comparative analysis, analytical diagnostics, forecasting and statistical, regression and correlation data analysis, and dialectical and regulatory methods^(20,21) Applying the dialectical method allowed the author to analyse the electronic document management system in the European Union, which is one of the critical elements of e-government, resulting in new knowledge about the content and ideas of this system, which opens up new opportunities for optimising government processes.

Analytical diagnostic methods allowed us to analyse the dynamics and level of development of digital technologies in the EU countries. The regulatory and legal method made it possible to collect and analyse in detail several legal acts regulating the field of electronic document management and cybersecurity, as well as the field of electronic justice, which made it possible to identify gaps and contradictions in the existing legislation, as well as to determine trends in its development⁽²²⁻²⁴⁾

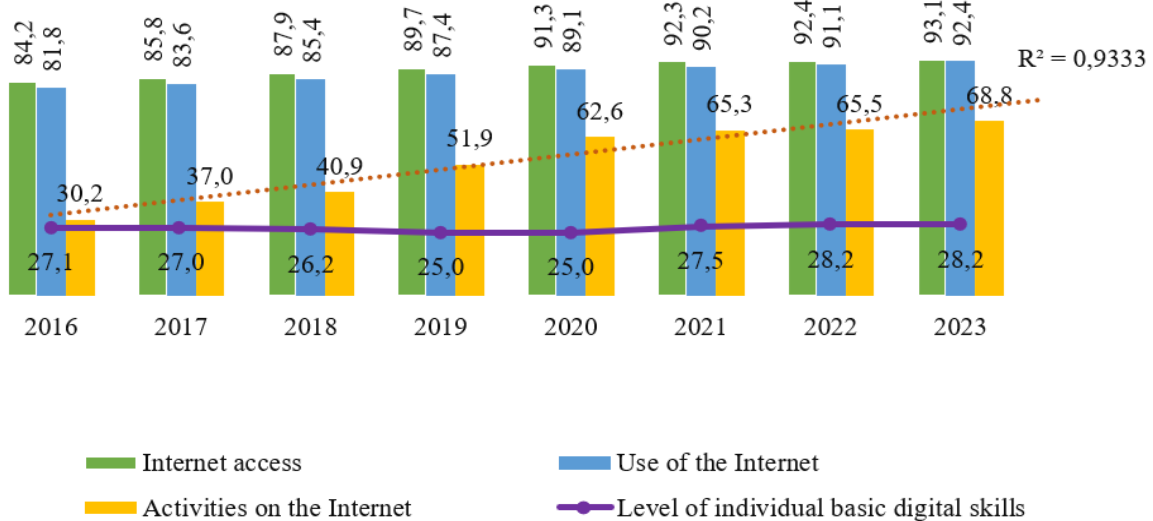
RESULTS

The constant increase in data volumes calls into question the effectiveness of traditional data processing methods, stimulating the development of new technologies; data analytics provides a competitive advantage, allowing for more informed decisions and adaptation to market changes.⁽²⁾

Digital transformation is an integral part of the European Union's strategic goals. The European Parliament plays a crucial role in shaping European policies aimed at developing the digital economy, ensuring the

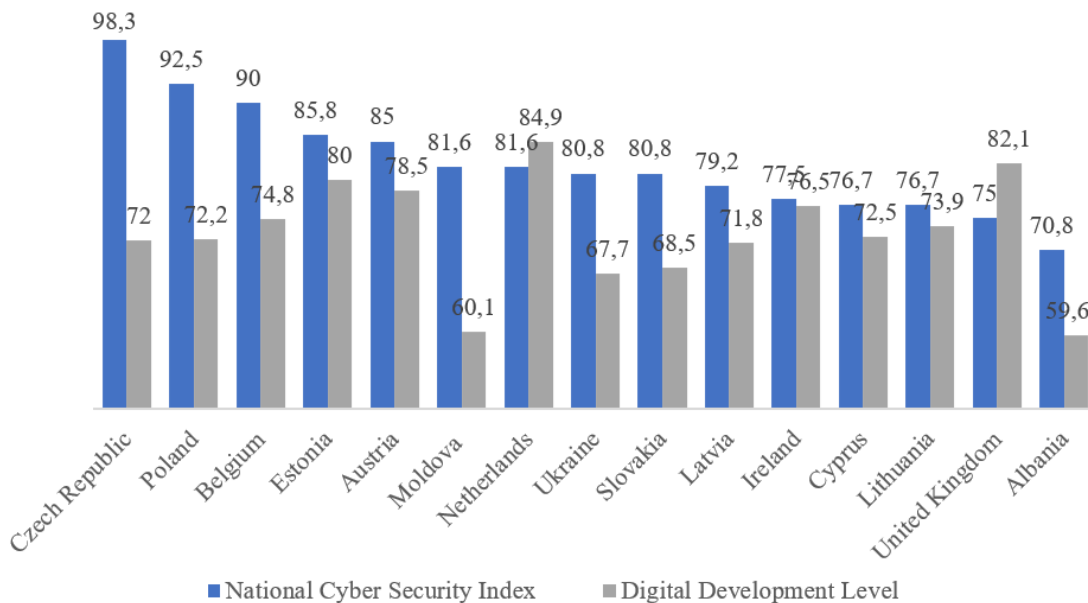
harmonious coexistence of humans and nature, and working to create a favourable environment for innovation, supporting digital education and the transition to digital public services, always in line with European values. The Digital Europe Programme (2021-2027) aims to make digital transformation accessible to all. It includes a set of measures to ensure that the benefits of the digital era are felt by individuals, businesses, organisations and public institutions alike.⁽²⁵⁾

According to open data from Eurostat⁽²⁴⁾, even though the digital divide between EU countries still exists, there is a positive trend towards its reduction due to significant investments in the development of broadband, mobile networks and other critical elements of digital infrastructure, as well as the implementation of policies aimed at ensuring digital accessibility (figure 1). The results of the regression analysis suggest that the degree of online activity of the adult population of EU countries has a reasonably high tendency to grow steadily in the future. The high correlation coefficient (0,98) between Internet access, use and activities confirms this trend.



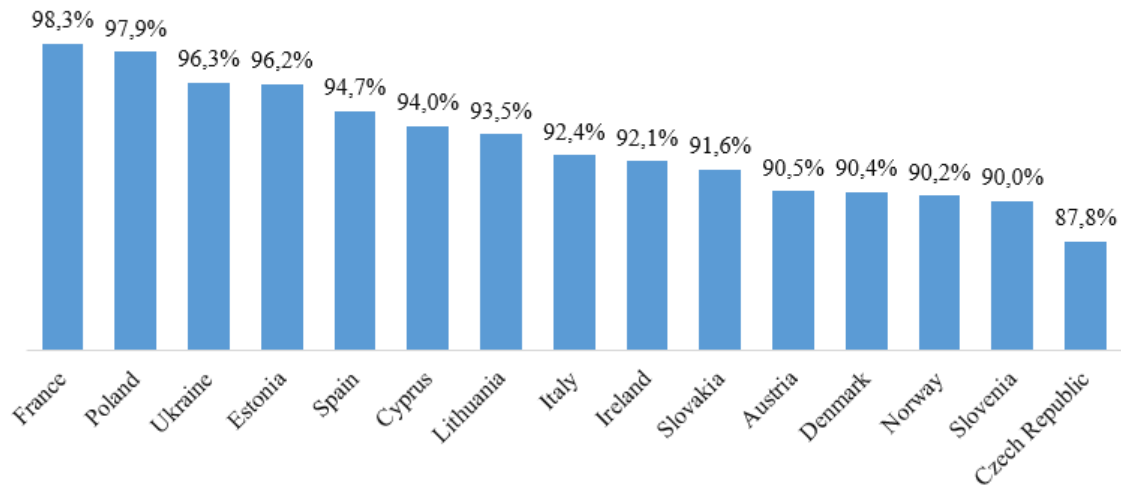
Source: compiled by the author based on data from Eurostat⁽²⁴⁾
 Figure 1. Indicators of the EU countries digitalisation level in 2016-2023

A systematic assessment of the level of cybersecurity is an integral part of national security, as it allows for a timely response to cyber threats, enhances the resilience of information infrastructure and contributes to the successful development of digitalisation.⁽²⁶⁾ A systematic approach to cybersecurity, including investment, cooperation and legislative changes, has allowed European countries to effectively counter cyber threats and maintain a high level of cybersecurity (figure 2).



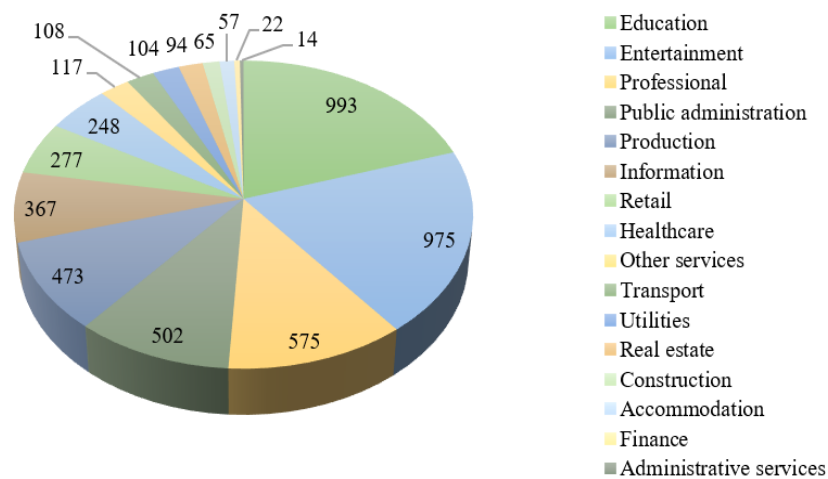
Source: based on data from Digital Decade DESI visualisation tool⁽²⁷⁾
 Figure 2. European countries with the highest level of cybersecurity compared to digital development, as of August 2024

The Open Data Ranking⁽²⁸⁾ which considers indicators such as data availability, quality and usage, is an essential indicator of a country’s digital potential. According to the data for August 2024 (figure 3), France is the leader in open data, providing the most significant public access to government information and creating a developed ecosystem for its use. Poland ranked second, has demonstrated significant progress in implementing an open data policy that includes expanding access to information and creating tools for its analysis and use. Despite the challenges of wartime, Ukraine’s significant efforts to open up data allowed it to become one of the top three. In digital transformation, when information becomes one of the most valuable resources, legal protection of information security plays a key role, guaranteeing its confidentiality and integrity.⁽⁷⁾



Source: based on Open Data in Europe 2023⁽²⁹⁾
Figure 3. Overall ranking of Europe’s leading countries by Open Data maturity indicator for 2023

Cyber-attacks threaten many industries, including energy, manufacturing, logistics, telecommunications, and software development, but most of all, they threaten government and government organisations (figure 4). According to Industries Most Targeted by malware global 2023⁽³⁰⁾ cyber threats in 2023 most affected the following industries in the European Union: manufacturing due to the widespread use of vulnerable industrial control systems and the value of data, finance and insurance due to the processing of large amounts of financial information and personal data, services due to the diversity of services and large amounts of data, energy due to critical infrastructure and data value, and retail due to large customer databases.^(31,32) These industries have become vulnerable due to the significant financial resources that can be gained from attacks, the large volumes of valuable data, critical infrastructure, and the complexity of their security systems. The findings show that although countries have achieved a certain level of cyberspace security, specific vulnerabilities in the cybersecurity system require technical remediation and improved legal regulation.

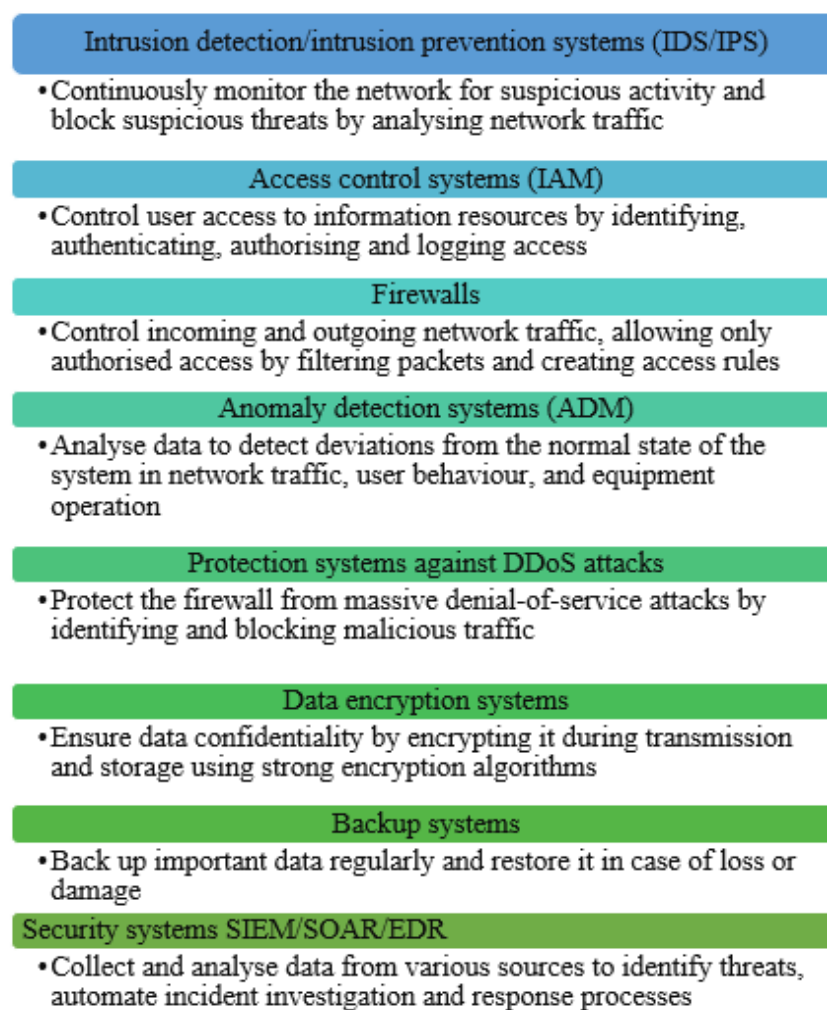


Source: Industries most targeted by malware global 2023⁽³⁰⁾
Figure 4. The most vulnerable sectors to cyberattacks in 2022-2023, units

Among the documents regulating the cybersecurity of EU networks and information systems, a special place is occupied by the NIS Directive, aimed at improving the overall level of security; the Critical Infrastructure Directive, which focuses on the protection of essential facilities; and the Convention on Cybercrime, which defines the legal framework for combating cybercrime. In order to strengthen cybersecurity at the level of member states, in 2016, the European Union introduced mandatory requirements for the adoption of national legislation in the field of network and information systems security, which included the establishment of competent authorities, identification of essential service providers and establishment of precise requirements for their security and incident reporting procedures. To create a digital single market, the EU has introduced a new cybersecurity certification system for ICT products and services to ensure high cyber resilience and trust in digital products and services.^(33,34) It ensures confidence in the safety and reliability of products that adhere to European cybersecurity norms. Given this risk, organisations must establish and maintain adequate cybersecurity measures for their digital infrastructure in the NIS Directive that consider identified risks and potential consequences to customers which could affect a large part of society (widely used services).

The NIS Directive seeks to promote cooperation at the international level, not only as a set of requirements for operators on reporting incidents and creating platforms for information exchange between member states and Europe. It can then respond more quickly and effectively to cyber threats, which has the potential to increase cybersecurity significantly. ENISA now has a lot more muscle, which means that it cannot be ignored in terms of its role as an influential player when formulating cybersecurity policy in Europe.

The agency develops strategies, encourages cooperation between member states, and supports cybersecurity at different levels. The content of these legal documents shows that protection against cyber threats is provided above all by a set of digital tools, which means that technical protection requires constant security training for staff (figure 5).



Source: compiled and supplemented by the author based on Khan A. et al ⁽³⁶⁾

Figure 5. Digital Cybersecurity Tools

The organisation's field of activity affects how successful, in general terms, a digital transformation is and its

results. Electronic document management is integral to modern digital transformation, allowing organisations to enhance efficiency, transparency, and competitiveness. This is a crucial element of modern digitalisation, which involves replacing paper documents with electronic counterparts and automating all processes related to creating, processing, storing, and transmitting documents. Such digitalisation significantly simplifies work processes, increasing the efficiency and transparency of organisations.⁽³⁵⁾ Automation avoids time-consuming manual operations, significantly increasing the efficiency and reliability of tasks, thus ensuring smooth cooperation between all parties involved and positively impacting productivity.

Modern electronic document management systems must comply with legal requirements and consider specific requirements for certain categories of documents that must be stored on paper under current legislation, which requires organisations to develop hybrid document management models. As early as the 1950s, public international law allowed electronic document exchange and attempted to legalise the relevant terms. The concept of an “electronic document” was first enshrined in international law by the 1952 UN Convention, which was aimed at improving international communication and introduced the term “information message”, which can be seen as the first step towards defining an electronic document.

To promote understanding between peoples, the treaty defines a “news report” as material typical for news agencies to convey information to the general public.⁽³⁷⁾ Adopted in 1996, the UNCITRAL Model Law on Electronic Commerce defined “data in the form of a message” as any information collected, processed, transmitted or stored by electronic, optical or similar technologies. This concept covers various communication media, from e-mail to telefax.

Electronic document management is a critical interaction element between citizens and the state within the e-government framework. The majority of citizens’ appeals are processed through the exchange of electronic documents. However, it is essential to understand that each electronic document must meet clearly defined legal requirements to ensure its legal force and effectiveness. Unlike paper documents, electronic documents have several peculiarities: they are software-dependent, can contain various types of data and can be changed without changing their content, making them more flexible and adaptable. One of the problems with electronic document management is the fragmentation of electronic documents and their dependence on external resources, which creates data loss risks, compromising the document’s integrity and complicating its long-term storage. Moreover, physical media for storing electronic documents have a limited lifespan and can be subject to damage.⁽³⁸⁾

The main goal of electronic document management systems is to automate the entire lifecycle of electronic documents - from creation to archiving. These systems in government agencies are directly used to improve quality and user efficiency by automating document flow, for example, decrees, orders, and reports. It helps cut down the bureaucratic process and fastens well-reasoned decisions, too. In the context of electronic document exchange, legislation defines the rights and obligations of authors who exercise those rights to signatories or recipients as well as intermediaries participating in such a process. They integrate all systems, including the software stored in it and standard operating procedure to subject incoming documents with document processing of house for they can optimise this storage system, which will be their quality and preserving this type as these ways are good.⁽³⁹⁾

The countries of the European Union are actively introducing e-document management. For instance, the Makadetepi Asi Pronounced Eisigopis Rieh Mapadetepi Deepfur law of Germany now permits the use of digital versions of document carriers to matter (instead of traditional form-based carrying paper) in the judicial system. It makes the court process speedier by switching to electronic copies of documents, giving all interested persons access to these accountings, and enabling fictitiaries to upload documents electronically. The introduction of electronic document management in the Bundestag has been an excellent achievement for environmental protection, as it prevented large paper production.

It was 2001 in Germany when the requirement for licensed signatures disappeared, allowing competition to start. At the same time, to increase confidence in electronic documents, the law establishes requirements for using a qualified electronic signature in some instances, for example, when concluding contracts in electronic form. Belgium became one of the first countries to implement fully electronic court proceedings, demonstrating global leadership in the digital transformation of justice. The country has adopted a law that created the legal basis for fully electronic court proceedings.

From now on, all participants in the judicial process can interact with each other electronically, and cases will be conducted exclusively in electronic form from start to finish. The Austrian state apparatus has developed an integrated system that covers the entire process of working with electronic documents - from their creation to final destruction- allowing for effective document management at all stages. France was one of the first countries to recognise the legal force of electronic documents and signatures at the legislative level. In 2000, a law that legalised using electronic documents in office work was passed. In 2001, a new electronic signature standard was introduced to guarantee the confidentiality and integrity of data.⁽³⁵⁾

Organisations such as the United Nations Commission on Enterprise, Business Facilitation and Development

(which focuses on business process facilitation), the United Nations Commission on International Trade Law (which regulates the legal aspects of international trade), the Centre for International Trade Facilitation of the Economic Commission for Europe (which specialises in trade facilitation in Europe) and the International Telecommunication Union (which sets standards for the use of electronic communications) have made significant contributions to the development of international rules and recommendations on electronic document management.^(40,41)

The initiation of new rules for electronic document management in finance is usually entrusted to international organisations such as UNCITRAL and the Council of Europe. In 1997, the UN recommended countries use the UNCITRAL Model Law on Electronic Commerce as a basis for national legislation. Thanks to the EU Directive on Electronic Commerce and other related documents, electronic documents have received the same legal status as paper documents, which has created a level playing field for electronic contracts, simplified procedures and made online interaction more reliable and secure.

According to UNCITRAL rules, the term “original” for an electronic document has a broader interpretation than for a paper document. If an electronic document fully preserves the information from the original file, then each copy of it can be considered an original. This means that, unlike paper documents, electronic documents may have several originals.⁽⁴²⁾

The introduction of an electronic document management system in the judicial area is critical in ensuring digitalisation justice, making judging processes more efficient and transparent. This and access to electronic justice, including laying down the acceptance of applications outside personal appointments and having consideration through video conferencing technologies, substantially reduced terms of considering cases, which expands the sphere for citizens in getting fair trials. The application of electronic justice is part of a broader judicial reform to improve efficiency, transparency and efficacy. Because of projects like the Unified State Register of Court Decisions, it is now possible for citizens to access court information on the Internet.

E-Justice is a component of E-Democracy, which promotes more significant opportunities and broader access for citizens to justice - a fundamental right in any democratic society. The introduction of electronic justice allows judicial services to residents of remote areas, which is lifesaving for a fair society and the concept of equal rights. Electronic justice in Ukraine is an effective system that allows participants to perform procedural actions as indicated by the code of law (in particular, according to a set Legislation - on Accesses (*) judicial decisions Act; Advocates and advocacy activities Law of Ukraine “On the Judiciary and the Status of Judges”).⁽⁴³⁾

For courts, electronic justice could automate many court procedures, enabling more efficient processing. These are, for example, the use of electronic document management systems and a videoconferencing system to support activities by courts and law enforcement agencies, creating e-archives - all sorts of standard innovative solutions which should allow for improving public administration in these areas. The shift to e-justice is a new window of opportunities and an effective method since it has several advantages over the traditional way. These benefits, such as the aforementioned automation of repetitive processes, an enhanced functioning of courts, and thus a more transparent process with broader access to justice, contribute to better quality judgments. Through online attendance by the general public to view hearing footage, judicial practices are made known for their transparency and integrity.⁽⁴⁴⁾

E-tools have provided for a better knowledge of legislation by citizens who can protect their rights abroad more rapidly and conveniently, while data exchange with the business registries has greatly facilitated procedures in lending since banks could carry out an instant financial status assessment of potential clients and thus mitigated risks. The application of electronic justice faces many issues, complicating the establishment of a mechanism for effective interaction among the participants in judicial proceedings. One of the primary hurdles to overcome before achieving full implementation is that many people in our country do not have access to and means for using modern digital communication tools, which creates an element electronic justice has yet to reach. Next, as society at large goes digital, the old-fashioned paper documentation must be done away with in favour of more up-to-date electronic formats.

Third, to effectively develop an electronic justice system, it must be high-security from a cyber threat point of view. Besides that, e-justice implementation is seriously hindered by the low level of digital literacy among many citizens. A solution to this issue is the need for federal programs on the development of digital literacy and also a change in primary education standards regarding credit of competencies in most populations using social networks.

DISCUSSION

Integrating digital technologies and the natural world makes it possible to build virtual models replicating real-world environments, providing an avenue for testing products or services. A combination of perpetual learning, innovation, and flexibility creates a competitive advantage for organisations by offering cost reductions, management process improvement, and legal security. AI, AR/VR, biometrics, and the cloud are the foundations of most modern digital transformations. While this is an advantageous transformation, it comes

with a unique set of obstacles – quick adaption to technology updates, more extraordinary security measures are required for cyber threats and managing large data volumes effectively.⁽⁴⁵⁾

The state is developing a strategy for shaping the single information space and its inclusion in the global context, as well as for forming IQ technologies based on the adaptability of existing legislation to new challenges associated with informatisation.^(5,46) This strategy will allow people to make much more informed decisions about the complex trade-offs between two bits of information or relationships and trends.

Intelligent analysis helps integrate heterogeneous data into a cohesive set/schema useful for making accurate predictions. These technologies have become general-purpose appliances for enhancing activities and automating the entire value chain from manufacture to services and are pertinent to the government.⁽⁹⁾ The application of artificial intelligence within Cybersecurity raises legal issues of bearing liability for autonomous system operations, copyright of the algorithm, and opaqueness in the decision-making process.⁽⁴⁷⁾

The institutional mechanisms the European Union provided and fruitful interaction with other countries of the EU, the business and international structures allowed creating and enacting the efficient policy of cyber surveillance, which has been able to counter the challenges posed by the digital space in the last three decades. At the dawn of the 21st century, the EU has focused on several strategies for the enhancement of cybersecurity, including formulation of a common political and legislative framework, establishment of cyber threat early warning systems, promotion of technology-related advances, improving the digital competencies of its citizens, standardisation and regulation of offensive and defensive cyber operational procedures.

The legal framework for electronic document management in the EU provides a solid foundation for creating a digital environment, but constant technological changes require constant legislation improvement. The EU continues to work towards a digital single market where electronic documents will have the same legal force as paper documents. The primary EU legislation in the field of electronic document management, such as Directive 1999/93/EC on electronic signatures, Directive 2000/31/EC on electronic commerce and Regulation (EU) No 910/2014 on electronic identification and trust services, defines the concept of electronic signatures, sets requirements for their creation and verification, and regulates legal aspects of e-commerce, in particular, those related to the conclusion of electronic contracts and ensuring trust in electronic transactions. The future of electronic document management in the EU is linked to further digitalisation and integration of various areas of life. New technologies, such as artificial intelligence, blockchain and cloud computing, open up new development opportunities. However, success requires the joint work of all stakeholders in cybersecurity and legislative adaptation.⁽¹⁸⁾

The introduction of e-justice in Europe, the United States, and Australia has simplified court procedures and minimised paperwork. Thanks to the European eJustice Strategy, first presented in 2008, EU courts are actively implementing electronic services such as electronic filing of documents, online court hearings and access to court registers via the Internet. The European e-Justice Portal allows citizens and businesses to file lawsuits, track case progress, and receive court decisions in electronic format without leaving home. In Ukraine, the implementation of electronic justice is a new hope in restructuring the judiciary, opening it for the public to access faster and more efficiently, albeit, its use is still limited.^(49,50)

The legal regulation of the digital space must be in a constant state of development to find the best possible equilibrium between progressive change and safeguarding the population's interests. Significant data concerns comprehensive engagement with a mass of data using unique technologies to find latent forms. In addition to fresh capabilities, advancing technologies also create new issues to be addressed in the form of data security and unfair competition, making a case for global laws which address competition prospectively while being able to create a conducive environment for investments in digital technologies and fostering creativity in firms.⁽⁵¹⁾

CONCLUSION

The advancement of the digital sphere brings about the transformation of classic legal relations and demands the establishment of new legal measures to regulate the applicable digital assets. There is a need to maintain an appropriate legal regime describing the rights and duties of the actors involved in their relationships owing to the new forms of interaction in the virtual environment. The execution of new legal instruments needs intimate collaboration between lawyers and other disciplines, including technology, commerce, and civil society.

The results of the study confirm the importance of legal support for electronic document management and computer security in the context of the digitalization of society. For successful digital transformation, it is necessary to implement an interdisciplinary approach that combines technical, managerial and legal measures. European experience, in particular the initiatives of the European Commission, indicates the importance of international cooperation in standardizing the legal aspects of electronic document management, although the challenges associated with adapting legislation to technological changes remain.

In addition, the expansion of electronic document management, in particular through the integration of e-justice, contributes to increasing the efficiency of management, legal processes and interaction between participants in the digital environment. It is important to ensure that national legislation complies with

international standards, which will strengthen the legal framework for the effective functioning of the digital economy.

Thus, the rapid convergence of economic sectors and increased competition will require constant review of the regulatory framework, especially in ensuring information security, combating cybercrime, and protecting the rights of citizens in the digital environment.

BIBLIOGRAPHIC REFERENCES

1. Boulton C. What is digital transformation? A necessary disruption. 2020. <https://www.cio.com/article/3211428/what-is-digital-transformation-a-necessary-disruption.html>
2. Buhrimenko R, Smirnova P. The impact of the development of digital transformation on the activity of the enterprise. *Economy and society*. 2024;(59). <https://doi.org/10.32782/2524-0072/2024-59-29>
3. Goldfarb A, Tucker C. Digital Economics. *Journal of Economic Literature*. 2019;57(1):3-43. <https://doi.org/10.1257/jel.20171452>
4. Pawełszek I, Kumar N, Solanki U. Artificial intelligence, digital technologies and the future of law. *Future Economics & Law*. 2022;2(2):24-33. <https://doi.org/10.57125/FEL.2022.06.25.03>
5. Bielialov T, Kalina I, Goi V, Kravchenko O, Shyshpanova N. Global Experience of Digitalisation of Economic Processes in the Context of Transformation. *International Journal of Professional Business Review*. 2023;8(6):e02041. <https://doi.org/10.26668/businessreview/2023.v8i6.2041>
6. Khaustova M. The concept of digitalisation: national and international approaches. *Law and innovations*. 2022;2(38):7-18. [https://doi.org/10.37772/2518-1718-2022-2\(38\)-1](https://doi.org/10.37772/2518-1718-2022-2(38)-1)
7. Bondarenko S, Makeieva O, Usachenko O, Veklych V, Arifkhodzhaieva T, LERNYK S. The Legal Mechanisms for Information Security in the context of Digitalisation. *Journal of Information Technology Management*. 2022;14(Special Issue: Digitalisation of Socio-Economic Processes):25-58. <https://doi.org/10.22059/jitm.2022.88868>
8. Nurahman D. Cybercrime Policies: Juridical Evidence and Law Enforcement Policies. In: *Proceedings of The International Conference on Environmental and Technology of Law, Business and Education on Post Covid 19, ICETLAWBE 2020, 26 September 2020, Bandar Lampung, Indonesia, 2020*. EAI. <https://doi.org/10.4108/eai.26-9-2020.2302579>
9. Ismanto H, Gunarto G, Endah Wahyuningsih S. The Juridical Formulation of Hate Speech Cyber Crime and Its Law Enforcement Implementation. *Law Development Journal*. 2021;3(4):710. <https://doi.org/10.30659/ldj.3.4.710-718>
10. Siregar GT, Sinaga S. The law globalisation in cybercrime prevention. *International Journal of Law Reconstruction*. 2021;5(2):211. <https://doi.org/10.26532/ijlr.v5i2.17514>
11. Putri RA, Adolf H, Sidik J. Law Enforcement of Cyber Crime Jurisdiction in Transnational Law. In *4th Social and Humanities Research Symposium (SoRes, 2021)*. Atlantis Press;2022. <https://doi.org/10.2991/assehr.k.220407.039>
12. Syahril MAF. Cyber Crime in terms of the Human Rights Perspective. *International Journal of Multicultural and Multireligious Understanding*. 2023;10(5):119. <https://doi.org/10.18415/ijmmu.v10i5.4611>
13. Information technology - Security techniques - Guidelines for cybersecurity (ISO/IEC 27032:2012) [cited 2024 Oct 30]. <http://www.iso.org/standard/44375.html>
14. On the Basic Principles of Ensuring Cybersecurity of Ukraine: Law of Ukraine No. 2163-VIII from 2024 [cited 2024 Oct 30]. <https://zakon.rada.gov.ua/laws/show/2163-19#Text>
15. Kiu MS, Lai KW, Chia FC, Wong PF. Blockchain integration into electronic document management (EDM) system in construction common data environment. *Smart and Sustainable Built Environment*;2022. <https://doi.org/10.1108/sasbe-12-2021-0231>

16. Benmakhlof H, Chouaou A. Electronic document, information, and archive management systems in economic institutions: a descriptive study of the onbase system. *International Journal of Professional Business Review*. 2024;9(6):e4755. <https://doi.org/10.26668/businessreview/2024.v9i6.4755>
17. Davydiuk A, Potii O. National Cybersecurity Governance: UKRAINE. *National Cybersecurity Governance Series*. 2024. https://ccdcoe.org/uploads/2024/08/National-Cybersecurity-Governance_Ukraine_Davydiuk_Potii_2024.pdf
18. Orioque J, Pajaron S, Cabardo J. Contextualised Online Document Management System. *Journal of Innovative Technology Convergence*. 2024;6(1):65-74. <https://doi.org/10.69478/JITC2024v6n2a07>
19. Bouchoux DE. *Legal research and writing for paralegals*. 5th ed. Aspen Publishers, 2009.
20. On Information: Law of Ukraine No. 2657-XII from 2023 [cited 2024 Oct 30]. <https://zakon.rada.gov.ua/laws/show/2657-12#Text>
21. On the Protection of Information in Information and Telecommunication Systems: Law of Ukraine No. 80/94-BP from 2024 [cited 2024 Oct 30]. <https://zakon.rada.gov.ua/laws/show/80/94-вр#Text>
22. Alnakeep HT. Internet crimes to legal regulation. *International journal of health sciences*. 2022;6(s7):48856-48876. <https://doi.org/10.53730/ijhs.v6ns7.13683>
23. Fedorov M, Liakh V, Ionan V, Kuzmycheva N. Study of digital literacy in Ukraine. Ministry of Digital Transformation of Ukraine. 2023 [cited 2024 Oct 30]. https://osvita.diia.gov.ua/uploads/1/8800ua_cifrova_gramotnist_naselenna_ukraini_2023.pdf
24. Language selection. European Commission [cited 2024 Oct 30]. <http://surl.li/igvscq>
25. The Digital Europe Programme. Shaping Europe's digital future [cited 2024 Oct 30]. <https://digital-strategy.ec.europa.eu/en/activities/digital-programme>
26. Chilenovu Ogborigbo J, Sekinat Sobowale O, Iyere Amienwalen E, Owoade Y, Taiwo Samson A, Egerson J. Strategic integration of cyber security in business intelligence systems for data protection and competitive advantage. *World Journal of Advanced Research and Reviews*. 2024;23(1):081-096. <https://doi.org/10.30574/wjarr.2024.23.1.1900>
27. Digital Decade DESI visualisation tool [cited 2024 Oct 30]. <https://digital-decade-desi.digital-strategy.ec.europa.eu/datasets/desi/charts>
28. NCSI: The Open Data Ranking. Index [cited 2024 Oct 30]. <https://ncsi.ega.ee/ncsi-index/?order=rank>
29. Open Data in Europe 2023. data.europa.eu - The official portal for European data | data.europa.eu [cited 2024 Oct 30]. <https://data.europa.eu/en/publications/open-data-maturity/2023>
30. Industries most targeted by malware global 2023. Statista [cited 2024 Oct 30]. <https://www.statista.com/statistics/223517/malware-infection-weekly-industries/>
31. On the Protection of Personal Data: Law of Ukraine No. 2297-VI from 2024 [cited 2024 Oct 30]. <https://zakon.rada.gov.ua/laws/show/2297-17#Text>
32. State Service for Special Communications and Information Protection of Ukraine [cited 2024 Oct 30]. <https://cip.gov.ua/ua/news/zmina-taktik-cilei-i-spromozhnostei-khakerskikh-grup-uryadu-rf-ta-kontrolovanikh-nim-ugrupovan-prognozi>
33. On the mandatory copy of documents: Law of Ukraine No. 595-XIV from 2023 [cited 2024 Oct 30]. <https://zakon.rada.gov.ua/laws/show/595-14#Text>
34. Measuring digital development ICT Development Index 2023. ITU: Committed to connecting the world [cited 2024 Oct 30]. <http://surl.li/jmdmjw>

35. Kushybek S. International legal regulation of electronic document circulation. *Historia i Świat*. 2021;(10). <https://doi.org/10.34739/his.2021.10.18>
36. Khan AA, Laghari AA, Li P, Dootio MA, Karim S. The collaborative role of blockchain, artificial intelligence, and industrial Internet of Things in the digitalisation of small and medium sized enterprises. *Scientific Reports*. 2023;13(1). <https://doi.org/10.1038/s41598-023-28707-9>
37. Convention on the International Law of Refutation, United Nations Convention, 1952 [cited 2024 Oct 30]. https://zakon.rada.gov.ua/laws/show/995_319#Text
38. Ghareeb AM, Darwish NR, Hefney HA. E-government adoption: a literature review and a proposed citizen-centric model. *Electronic Government, an International Journal*. 2019;15(4):392. <https://doi.org/10.1504/eg.2019.102592>
39. Wirtz BW, Kurtz OT. Local e-government services: quality aspects and citizen usage preferences. *Electronic Government, an International Journal*. 2018;14(2):160. <https://doi.org/10.1504/eg.2018.090928>
40. On Electronic Communications: Law of Ukraine No. 1089-IX from 2024 [cited 2024 Oct 30]. <https://zakon.rada.gov.ua/laws/show/1089-20#Text>
41. On State Secrets: Law of Ukraine No. 3855-XII from 2024 [cited 2024 Oct 30]. <https://zakon.rada.gov.ua/laws/show/3855-12#Text>
42. Commission Sessions | United Nations Commission on International Trade Law. United Nations Commission on International Trade Law [cited 2024 Oct 30]. <https://uncitral.un.org/en/commission>
43. On the Judiciary and the Status of Judges, Law of Ukraine No. 1402-VIII from 2024 [cited 2024 Oct 30]. <https://zakon.rada.gov.ua/laws/show/1402-19#Text>
44. On the Bar and Practice of Law: Law of Ukraine No. 5076-VI from 2023 [cited 2024 Oct 30]. <https://zakon.rada.gov.ua/laws/show/5076-17#Text>
45. Chmeruk H. Tools for digital transformation of business entities. State and regions. Series: Economics and Business. 2020;2(113). <https://doi.org/10.32840/1814-1161/2020-2-29>
46. On the Strategy for the Development of the Justice System and Constitutional Justice for 2021-2023: Decree of the President of Ukraine No. 231/2021 from 2021 [cited 2024 Oct 30]. <https://zakon.rada.gov.ua/laws/show/231/2021#Text>
47. Cardoza C, Wagh R. A text analysis framework for understanding cyber-crimes. *International Journal of advanced and applied sciences*. 2017;4(10):58-63. <https://doi.org/10.21833/ijaas.2017.010.010>
48. European e-Justice Portal [cited 2024 Oct 30]. <https://e-justice.europa.eu/>
49. On Access to Court Decisions: Law of Ukraine No. 01-8/195 from 2006: Letter of the Supreme Economic Court of Ukraine [cited 2024 Oct 30]. <https://zakon.rada.gov.ua/laws/show/va195600-06#Text>
50. Decision - 2011/833 - EN - EUR-Lex. (n.d.-b). The official portal for European data | data.europa.eu. <http://data.europa.eu/eli/dec/2011/833/oj>
51. Orlova OS. Legal regulation of economic activity in conditions of digitalisation. *Bulletin of the Uzhhorod National University. Series: Law*. 2023;1(77):195-201. <https://doi.org/10.24144/2307-3322.2023.77.1.31>

FINANCING

The authors did not receive financing for the development of this research.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest.

AUTHORSHIP CONTRIBUTION

Conceptualization: Valentina Petrovich.

Data curation: Oleksandr Alosyn.

Formal analysis: Lidiia Moskvych, Nataliia Shcherbakova.

Research: Lina Doroshenko.

Methodology: Valentina Petrovich.

Project management: Valentina Petrovich.

Resources: Lidiia Moskvych, Nataliia Shcherbakova, Lina Doroshenko.

Software: Lidiia Moskvych, Nataliia Shcherbakova, Lina Doroshenko.

Supervision: Valentina Petrovich.

Validation: Lina Doroshenko.

Display: Oleksandr Alosyn.

Drafting - original draft: Oleksandr Alosyn.

Writing - proofreading and editing: Oleksandr Alosyn.