African Journal of Applied Research
Vol. 11, No. 1 (2025), pp. 173-193
http://www.ajaronline.com
https://doi.org/10.26437/ajar.v11i1.
Received: August 25, 2024
Peer reviewed: October 30, 2024
Revised: December 12, 2024
Published: January 2025

THE TRANSFORMATION OF LEGAL FRAMEWORKS THROUGH SECURE DIGITISATION

Savchenko, V.[1], Podolieva, A.[2], Olkhovskyi, O.[3], Halona, I.[4] and Aloshyn, O.[5]
[1]*Department of Civil-Legal Disciplines, Law Faculty, V. N. Karazin Kharkiv National University, Kharkiv, Ukraine.*
[2]*Department of Law and Law Enforcement, Zhytomyr Polytechnic State University, Zhytomyr, Ukraine.*
[3]*Department of National Security, Public Management and Administration, Zhytomyr Polytechnic State University, Zhytomyr, Ukraine.*
[4]*Department of Transport Technology, National Transport University, Kyiv, Ukraine.*
[5]*Interregional Academy of Personnel Management, Kyiv, Ukraine.*
[1]*savchenko.viktor@gmail.com*

ABSTRACT

Purpose: This research article aims to study the positive and negative factors in implementing electronic document management, analyse the legal aspect of its functioning in the international context, and identify gaps in ensuring cybersecurity.

Design/Methodology/Approach: The research methodology was developed using a mixed approach. The qualitative aspect of the study included literature analysis, comparative analysis, statistical data analysis, generalisation, and systematisation, and the quantitative aspect assessed the impact of digital innovations on cybersecurity risks. A survey of legal experts (total = 16 participants) was conducted. The results were interpreted by correlation analysis conducted in the JASP statistical software using Pearson's Correlations tool.

Research Limitation: The study's main limitation is its focus on the domestic problems of implementing electronic document management in the context of rapid digital transformation.

Findings: The study found that electronic document management will mainly increase productivity by simplifying the basic processes of searching, editing, storing, and sharing digital documents. This will increase the availability of digital information, which, at the same time, will increase the risk of cyber terrorism.

Practical Implication: The study provides industries with actionable insights on optimising workflows, reducing operational costs, and mitigating cybersecurity risks through secure and efficient electronic document management.

Social Implication: The research results point to gaps in the modern electronic document management system, which is beneficial to society and provides the opportunity to increase transparency and trust in government institutions by improving the efficiency and security of document management systems.

Originality/Value: The study expands the scholarly discourse on digital governance by aligning technological progress with international legal standards and cybersecurity practices, thus bridging the gap between theory and practice in digital transformation research.

Keywords: *Digital. cybersecurity. cyberterrorism. e-governance. legal relations*
ISSN: 2408-7920

African Journal of Applied Research
Vol. 11, No. 1 (2025), pp. 173-193
http://www.ajaronline.com
https://doi.org/10.26437/ajar.v11i1.
Received: August 25, 2024
Peer reviewed: October 30, 2024
Revised: December 12, 2024
Published: January 2025

INTRODUCTION

In the context of creating and implementing the components of the digital industry, also known as Industry 4.0, a priority for many developed countries is to ensure the conditions for the introduction and promotion of competitive digital technologies, which allows them to spread their influence on the global political and economic environment. 2022 the global Industry 4.0 market was estimated at USD 113.86 billion. It is expected to reach USD 516.69 billion by 2031. It is expected to reach USD 116.69 billion by 2021, showing a CAGR of 18.38% over the next ten years (Straits Research, 2024).

The development of Industry 4.0, which is characterised by the active integration of intelligent technologies into all spheres of public life, has become the basis for forming electronic document management as an integral part of modern legal relations. Digital innovations, such as business process automation, artificial intelligence technologies, Big Data, and blockchain, which became widespread as part of the Industrial Revolution, are contributing to a fundamental change in the modern system of creating, transferring, and storing documents.

The widespread use of electronic document management in many countries and individual organisations increases the efficiency of management processes, reduces time and resources, and ensures high accuracy and transparency in business records. Abacı and Medeni (2022) confirm the need to improve electronic document management systems, given the expectation of improved service (40.9%) and the quality and richness of information (26.2%) of the 880 business representatives surveyed, who cited a lack of technical infrastructure as a barrier to its implementation.

However, the digital transformation of internal government processes, especially the document management system, has made it essential to ensure a robust cybersecurity policy, given the growing risks of confidential information leakage and cyber-attacks. In this context, it is worth noting that in the second quarter of 2024, Check Point Research (2024) recorded a 30% year-on-year increase in the number of cyber-attacks worldwide, reaching 1636 attacks per organisation per week, with government agencies being at the highest risk, currently experiencing 2084 attacks per week, along with education (3341 attacks per week) and healthcare (1999 attacks per week).

This trend is driven by various reasons, ranging from the ever-increasing digital transformation to new methods of cybercrime that use advanced techniques such as artificial intelligence and machine learning. In this context, the study of the legal aspects of the implementation of electronic document management and the relevant cybersecurity policy becomes necessary to ensure the resilience of the state and individual organisations to new threats of the industrial revolution.

ISSN: 2408-7920

African Journal of Applied Research
Vol. 11, No. 1 (2025), pp. 173-193
http://www.ajaronline.com
https://doi.org/10.26437/ajar.v11i1.
Received: August 25, 2024
Peer reviewed: October 30, 2024
Revised: December 12, 2024
Published: January 2025

The main limitation of this study is the use of only available theoretical and statistical sources in analyzing electronic document flow, which could limit its depth in terms of empirical verification of conclusions. It should also be noted that the issue of cybersecurity in electronic document management was considered in the article with an emphasis on general principles and tools that do not always consider the specifics of individual industries or unique threats associated with different types of information systems.

This article aims to assess the impact of digital innovations on legal relations, electronic document management, and cybersecurity. It highlights the positive and negative aspects of introducing electronic document management and analyses its legal aspects internationally. The article identifies the processes that accompany electronic document management's cybersecurity. In addition, this article assesses the impact of digital innovations on cybersecurity risks.

LITERATURE REVIEW

In the context of Industry 4.0 development, digitalisation is a crucial factor that creates productivity, profitability and economic growth for enterprises in all sectors of the economy. Modern research emphasises that enterprises that promote development and actively implement digital technologies have significant advantages in adapting to change and increasing their efficiency (Bielialov et al., 2023; Rüßmann et al., 2015; Warner & Wäger, 2019; Zhang et al., 2023). In addition, in global digitalisation, the state needs to engage and adapt state institutions to change and focus on building a new type of society (Ortina et al., 2023).

In this context, the quality of digitalisation at the state level is a crucial aspect of e-government implementation. This will contribute to increasing the transparency, efficiency, and accessibility of public services for citizens (Krysovatyy et al., 2024; Krasnykov et al., 2024), for example, by reducing administrative barriers, simplifying document creation procedures, and facilitating access to information about government programmes (Zhang & Kaur, 2024).

Electronic document management, as a component of the e-government mechanism, significantly changes legal relations, according to Abacı and Medeni (2022), due to improving communication processes between different interacting entities. Asogwa (2013), Gruzd and Yermolenko (2023), Kouroubali and Katehakis (2019), Orazgaliyeva et al. (2023) note that communication is improved by simplifying access to public services, corporate and personal documentation and information resources, which ensures transparency and efficiency in interaction with citizens (users of public services) or consumers of company products.

Several modern authors also note its effectiveness in terms of reducing the time for basic operations (Di Marzo Serugendo et al., 2024), availability of electronic versions of documents

African Journal of Applied Research
Vol. 11, No. 1 (2025), pp. 173-193
http://www.ajaronline.com
https://doi.org/10.26437/ajar.v11i1.
Received: August 25, 2024
Peer reviewed: October 30, 2024
Revised: December 12, 2024
Published: January 2025

for automated processing (Benmakhlouf & Chouaou, 2024) and reduction of resource requirements (Abidin & Husin, 2018). Given these aspects of electronic document management, it should be noted that it is a functional replacement for traditional methods of processing paper-based documents that are inefficient and show insufficient efficiency in the face of the urgent need for speed and an increase in the volume of processed documents due to the growth of information (Nagy, 2016; Pappel et al., 2020; Kussainova et al., 2020).

In addition, the introduction of digital innovations and electronic document management still lack a single effective legal regulation mechanism, so it is necessary to develop regulations that provide a legal framework for protecting electronic documents from cybercrime and fraud schemes, as well as mechanisms of liability for their violation (Bondarenko et al., 2022; Poliakov, 2023). It is also essential to introduce a set of technological and organisational measures aimed at protecting electronic documents, including a data encryption system (Rawat et al., 2019), authentication and authorisation when interacting with data (Pritee et al., 2024), physical security elements (e.g., access control systems for premises) (Shvets, 2019), monitoring and auditing of user activity and events in the system (Poliakov, 2023).

METHODOLOGY

The research methodology was developed within the framework of a mixed approach using both qualitative and quantitative analysis methods. The qualitative aspect of the research included a literature review to identify the positive and negative aspects of the introduction of electronic document management, a comparative analysis to study the legal aspects of the introduction of electronic document management in countries with different levels of digitalisation, analysis of statistical data to analyse the volume of cyber-attacks in different sectors of the economy. Methods of generalisation and systematisation to identify tools for preventing and eliminating the consequences of cybercrime and politically motivated attacks.

We used the expert evaluation method to collect primary data for quantitative analysis. The survey was conducted among the academics of the Department of International and European Law (Group 1 – 10 professors) and the Department of Law and Public Administration (Group 3 – 6 professors). The selection of experts was conducted using the targeted selection of candidates based on the expert's knowledge and overall self-assessment of his or her competence in solving the task. As a result of evaluating the factors using the “AVERAGE” function in the Exel analysis package, weighted average scores for each indicator were calculated. The functionality of the JASP statistical software was used to identify the correlation between the identified factors. This allowed us to determine the degree of correlation between the two measurement variables: the advantages and disadvantages of electronic document management and the consequences of cyber risks.

African Journal of Applied Research
Vol. 11, No. 1 (2025), pp. 173-193
http://www.ajaronline.com
https://doi.org/10.26437/ajar.v11i1.
Received: August 25, 2024
Peer reviewed: October 30, 2024
Revised: December 12, 2024
Published: January 2025

FINDINGS AND DISCUSSION

The rapid development of digitalisation phenomena as part of the fourth industrial revolution is shaping new models of management, interaction and organisation of activities in all sectors of the economy. In this context, electronic document management is emerging as a response to the demands of the times, when traditional methods of processing paper-based documents are proving to be inefficient in the face of the urgent need for speed and an increase in the volume of processed documents due to the growth of information.

The electronic document management market dynamics are proliferating and have an average annual growth rate of 14.47% (Figure 1). Thus, electronic document management, which involves creating, editing, signing, registering, storing and transmitting documents in digital form, allows organisations to effectively manage, store, share and collaborate on documents in a digital environment (Pasichnyk et al., 2024).

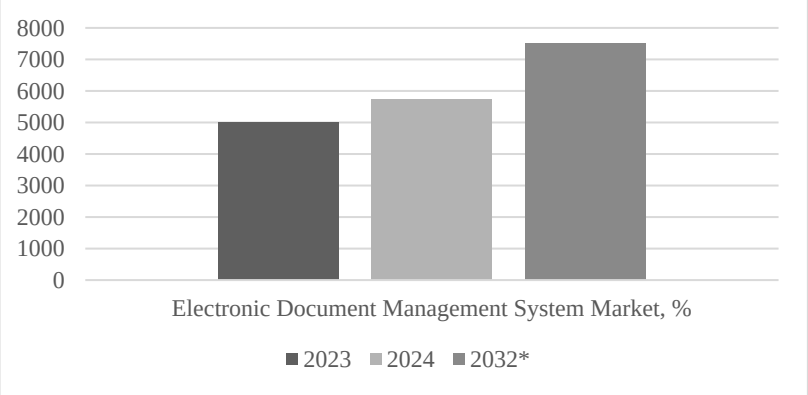

Figure 1: Market Size of Electronic Document Management Systems
Source: Global Growth Insights (2024)
*Note: * – forecast values*

Currently, the most common electronic documents are text files containing textual information in characters, verbal expressions and sentences. This type of documentation is the basis for many types of information exchange and comes in several standard formats, including DOCX, TXT, PDF, RTF and HTML. In addition, some electronic documents are intended to be presented as organised data in table files in XLSX, CSV and ODS formats. Typical formats for images in electronic documents are JPEG, PNG, GIF and TIFF, which are used when graphic images, such as photographs, drawings or diagrams, are required in a document. Also, some electronic documents may contain audio and video files (e.g., soundtracks, videos) in MP3, WAV, MP4, and AVI formats that can be played using appropriate software or media devices (Boiko, 2024).

ISSN: 2408-7920

African Journal of Applied Research
Vol. 11, No. 1 (2025), pp. 173-193
http://www.ajaronline.com
https://doi.org/10.26437/ajar.v11i1.
Received: August 25, 2024
Peer reviewed: October 30, 2024
Revised: December 12, 2024
Published: January 2025

Analysis of the positive and negative aspects of implementing electronic document management

The key benefits of the widespread use of electronic document management in the reporting of public authorities, municipalities and other government agencies, as well as in the business sector, are increased productivity, mainly due to the simplification of the processes of searching, editing, storing and exchanging digital documents.

The result of this optimisation is a reduction in the time required to perform basic operations, which directly impacts the performance of organisations. At the same time, improving communication processes between various interacting entities (internal and external environment of the organisation) by simplifying access to public services and information resources ensures transparency and efficiency in interaction with citizens (users of public services) or consumers of the company's products. It is also worth noting the availability of electronic versions of documents for automated processing through information systems, fast transmission through communication networks, the ability to store large amounts of information and ease of editing and copying, and, in addition, the availability of digital signatures and authentication mechanisms that guarantee legal validity and ensures compliance with the standards of legal purity and data security.

In addition, a transparent system of legal regulation and high-quality implementation of electronic document management, mainly through encryption and secure storage in cloud services, significantly reduce the risks of loss or unauthorised access to confidential data of users of public services and clients of national enterprises.

In turn, the environmental efficiency of electronic document management is related to the interest in reducing the use of resources (paper, ink, printing devices) in the reporting of enterprises and reducing the costs associated with printing, storing and transporting paper documents. Thus, at the national and local levels, the rationalisation of costs and the preservation of the environment are being implemented. In this context, as part of the state's sustainable development goals, the distribution of electronic versions of documents not only reduces the resource component of the process but also increases their accessibility for people with limited mobility and people from remote regions. Instead, the following were identified as critical obstacles to the functioning and legal regulation of electronic document management:

i. The difficulty of determining the objects of legal regulation when implementing electronic document management arises from the inability to formulate priority areas and a transparent system of legal regulation in the context of the rapid development of digital technologies. In this context, the risk of losing the integrity of the legislative system arises due to replacing traditional legal norms with ad hoc and fragmented regulation, which slows the response to global economic and social trends.

ISSN: 2408-7920

African Journal of Applied Research
Vol. 11, No. 1 (2025), pp. 173-193
http://www.ajaronline.com
https://doi.org/10.26437/ajar.v11i1.
Received: August 25, 2024
Peer reviewed: October 30, 2024
Revised: December 12, 2024
Published: January 2025

ii. The absence of developed legal categories and terminology or their inconsistency with the practical realities of electronic document management leads to legal conflicts or inaccuracies in applying relevant regulations, deepening the lag between legislation and the development of digital innovations.

iii. The problem of legal regulation inertia manifests in the legal framework's inability to promptly cover all aspects of innovative technologies when they are extended to a large audience. In the long-standing context, prompt adaptation of legal regulation of electronic document management requires preliminary analysis and thorough research of stakeholder priorities to ensure that regulations meet public expectations; however, if the necessary legislation is delayed, the opposite effect on its effectiveness may be possible.

iv. The emergence of new security risks, such as confidential information leaks and cyber-attacks, in the absence of legal instruments to minimise them, requires the state to develop appropriate measures to ensure an optimal level of cybersecurity without hampering innovative development and protection of citizens' rights in the digital environment.

v. The need to develop new quality criteria for legislation, such as adaptability to technological changes, high level of cybersecurity, transparency and flexibility of legislation, etc., will help meet stakeholders' need to effectively regulate electronic document flow while preserving human rights and international reporting standards.

The absence of a favourable national jurisdiction in digital innovation makes it challenging to implement electronic document management due to the lack of adaptation of legal norms to the modern requirements of the digital economy. In this context, legal gaps are emerging that pose additional risks to parties to legal relations, in particular about data protection and the legitimacy of electronic signatures, and generally reduce the efficiency of electronic document management processes. At the same time, the problem of ensuring digital sovereignty, manifested in ensuring the quality and independence of control over national information systems, is the need to eliminate external influence on internal information exchange processes and thus guarantee the protection of confidential data and security in cyberspace.

Legal aspects of implementing electronic document management

The legal regulation of electronic document management aims to establish clear rules and standards governing the rights and obligations of the parties in the process of creating, processing, transferring and storing electronic information. In this context, legal regulation aims to ensure the security, confidentiality and integrity of electronic documents and, in addition, provides for the creation of a legal framework for the use of this type of documents

ISSN: 2408-7920

African Journal of Applied Research
Vol. 11, No. 1 (2025), pp. 173-193
http://www.ajaronline.com
https://doi.org/10.26437/ajar.v11i1.
Received: August 25, 2024
Peer reviewed: October 30, 2024
Revised: December 12, 2024
Published: January 2025

in various areas of public life, including business and administrative processes, legal relations, research.

A high level of development of legal regulation of electronic document management is observed in Estonia, where, for the first time in the world, the parliament was elected via the Internet, an electronic census was conducted, and an electronic residence for foreigners was introduced. In Estonia, document management is regulated by the Digital Signature Act (Digitaalallkirja seadus), which defines the main legal categories and gives electronic signatures the same legal force as traditional signatures (Riigikogu, 2000); The Law of Debt Act (Võlaõigusseadus), which recognises a document as valid if the parties with legal capacity reach an agreement, regardless of whether it is verbal, electronic or physical on paper (Riigikogu, 2001); and the Personal Data Protection Act (Isikuandmete kaitse seadus), which guarantees the confidentiality and security of personal information in the electronic exchange of documents (Riigikogu, 2018).

In addition, Estonia has one of the world's most developed systems of electronic identification through identification cards, which provides citizens with access to e-government services at any time and digital signature of any document (Pappel et al., 2017); as well as the aforementioned e-resident service, which in the long run may provide the country with an increase in the number of virtual companies, regardless of the nationality of the owners, doing business and paying taxes in Estonia, but the issue of the legality of resident rights has not yet been settled.

In contrast, Singapore's well-developed legal regulation of electronic document flow is provided mainly by the Electronic Transactions Act (Singapore Statutes Online, 2010), which regulates the legal aspects of electronic transactions, and the Personal Data Protection Act (Singapore Statutes Online, 2012), which provides control over the processing of confidential data. In contrast, Norway implements an adequate legal framework through the Lov om elektronisk kommunikasjon, which covers activities related to electronic communications and related equipment (Lovdata, 2003).

Although Norway is not a member of the European Union (EU), it has close ties with the EU through its membership agreements in the European Economic Area and the European Free Trade Association. As a result, the Electronic Identity and Trust Services Regulation for Electronic Transactions in the Internal Market (eIDAS) is fully incorporated into Norwegian law through the Electronic Trust Services Act (Lovdata, 2018). Additional provisions in the Regulation on Trust Services for Electronic Transactions (Forskrift om tillitstjenester for elektroniske transaksjoner) allow for the transposition of the European Commission's implementing acts in line with the eIDAS Regulation (Lovdata, 2019).

The average level of development of legal regulation of electronic document flow is inherent in the legislation of the United States and Canada. In particular, the United States, like many

ISSN: 2408-7920

African Journal of Applied Research
Vol. 11, No. 1 (2025), pp. 173-193
http://www.ajaronline.com
https://doi.org/10.26437/ajar.v11i1.
Received: August 25, 2024
Peer reviewed: October 30, 2024
Revised: December 12, 2024
Published: January 2025

other countries, gives legal force to electronic signatures under the Electronic Signatures for Global and National Commerce Act (E-SIGN Act), which legitimises electronic documents in business (FDIC, 2014). However, there are still discrepancies in different states' regulations, making it challenging to have a unified practice of using electronic document management. Instead, Canada provides a single, transparent system of legislation in the field of electronic document management contained in the Personal Information Protection and Electronic Documents Act (Government of Canada, 2000), which regulates the legal issues of electronic document management and ensures the protection of sensitive data.

The low level of development of legal regulation of electronic document management in developing countries is due to limited infrastructure and resources, as well as local political, economic or social challenges. For example, in Ukraine, which is in the midst of a protracted war, the practical implementation of existing regulations, such as the Laws of Ukraine "On Electronic Documents and Electronic Document Management" (VRU, 2003) and "On Electronic Digital Signature" (VRU, 2017), is often complicated by limited infrastructure and lack of proper control.

The main document regulating this issue is the Law of Ukraine "On Electronic Documents and Electronic Document Management", as it defines the legal equivalence of electronic documents, establishes requirements for the use of electronic signatures, mechanisms for their verification and rules and requirements for their storage; user rights regarding confidentiality and protection of personal data in such documents; and establishes the procedure for interaction between stakeholders through electronic documents. Despite the country's complex political and economic situation, the level of digitalisation is relatively high, and, therefore, the most significant problem in regulating related issues is the inertia of legal regulation. Instead, Mexico, in the context of the economic stratification of a large part of the population, needs to develop further the provisions of the Law on Electronic Communications and Trust Services (Ley de Firma Electrónica Avanzada), taking into account the gaps in transparency and security of electronic document flow (Cámara de Diputados, 2012).

Ensuring cybersecurity of electronic document management

In today's digital transformation environment, which fundamentally changes approaches to managing information flows, data processing and ensuring effective interaction within the state and individual organisations, the issue of electronic document management cybersecurity requires new approaches to preventing and addressing its consequences. In addition, the emergence of digital innovations is leading to an increase in the number and scale of cybercrime: while in 2020, the number of online crime cases was 15421, the total number of cyber-attacks is now significantly higher than before, reaching millions of incidents per year, including massive attacks on critical infrastructure and government agencies (Stouffer, 2022). The current distribution of cyber-attacks by different sectors of the economy is shown in Figure 2.

ISSN: 2408-7920

African Journal of Applied Research
Vol. 11, No. 1 (2025), pp. 173-193
http://www.ajaronline.com
https://doi.org/10.26437/ajar.v11i1.
Received: August 25, 2024
Peer reviewed: October 30, 2024
Revised: December 12, 2024
Published: January 2025

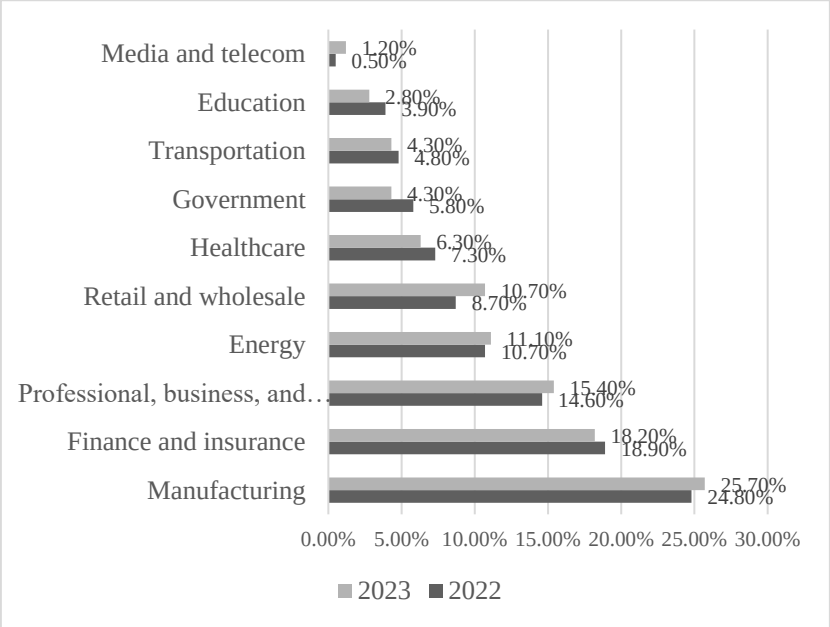

Figure 2: Share of Cyber Attacks in Global Industries in 2022–2023
Source: Petrosyan (2024)

Data security includes a set of technological and organisational measures to protect information resources from unauthorised access, alteration, deletion or damage. The following are among the most effective tools for preventing and eliminating the consequences of cyber-attacks:

i. The regulation of information systems, including electronic document management systems, is based on authentication, which involves the use of passwords, biometric data, and the implementation of multi-factor authentication, and authorisation, which involves verification and confirmation of users' rights to perform certain actions or access specific resources (Pritee et al., 2024).

ii. Physical data protection involves preventing threats to physical storage media, servers, and network equipment. It consists of introducing restrictions on physical access to servers and implementing special video surveillance and access control systems, which reduce the risk of unauthorised physical access to information or documents (Shvets, 2019).

iii. Systematic monitoring and implementation of the audit mechanism allow tracking the level of user activity and events in the system, which helps to respond quickly to possible security incidents and increases the level of data security (Poliakov, 2023).

ISSN: 2408-7920

African Journal of Applied Research
Vol. 11, No. 1 (2025), pp. 173-193
http://www.ajaronline.com
https://doi.org/10.26437/ajar.v11i1.
Received: August 25, 2024
Peer reviewed: October 30, 2024
Revised: December 12, 2024
Published: January 2025

iv. Implementation of international standards and legislation (e.g. GDPR in the European Union), which set high requirements for protecting personal data and information in electronic form.

Data encryption converts information into a secure code and thus allows you to ensure confidentiality and protect important documents during storage and transmission. This code can only be decrypted if the appropriate access code is available (Rawat et al., 2019).

It is also essential to consider the threat of the spread of organised cybercrime at the global level. In particular, an example of such crime is the Russian-Ukrainian cyber war, which is developing against the backdrop of Russia's armed aggression against Ukraine. As a result of Russia's systematic politically motivated cyber-attacks, the total number of cybercrimes has increased significantly, with 2693 such attacks recorded between 2000 and 2024, of which 1110 occurred in the military years of 2022-2024 (NetFreedom, 2024).

Politically motivated cyber-attacks targeting political targets and critical infrastructure, whether initiated by states (or their affiliated groups) or individual actors with political motives, have several negative consequences, including destabilisation of economic processes, disruption of public services, loss of trust in state institutions; compromise of data security; and obstacles to the free functioning of democratic processes.

In the case of modern cyberwarfare, Russian attacks have targeted energy infrastructure, the financial system and communication networks, with the Petya malware family being an example of the most extensive developments. Measures to prevent politically motivated cyber-attacks and eliminate the consequences of cyber warfare include the creation of a nationwide system of mechanisms for detecting cyber-attacks and countering acts of cyberterrorism and cyberespionage, the introduction of analytical and forensic support for the state's cybersecurity, the introduction of a counterintelligence protection system in the field of electronic communications, and the development of automatic real-time cyber-attack detection programmes. These measures also include improving the system's regulatory, legal, organisational and personnel support for combating cyberwarfare and cyberterrorism.

Assessing the impact of digital innovations on cybersecurity risks

It is assumed that the problems and prospects for introducing digital innovations into the electronic document management system previously identified in this paper positively impact the level of risk in the digital environment of organisations caused by the growing number of cyber-attacks. Therefore, in order to assess the impact of digital innovations on key aspects of cybersecurity, a survey was conducted among academics of the Department of International and European Law (Group 1 - 10 professors) and the Department of Law and Public Administration (Group 3 - 6 professors) on the significance of factors in the overall context of electronic document management (Appendix A).

ISSN: 2408-7920

African Journal of Applied Research
Vol. 11, No. 1 (2025), pp. 173-193
http://www.ajaronline.com
https://doi.org/10.26437/ajar.v11i1.
Received: August 25, 2024
Peer reviewed: October 30, 2024
Revised: December 12, 2024
Published: January 2025

As a result of processing the obtained values, the weighted average scores calculated using the Excel Analysis Package (AVERAGE function) for the criteria Increased productivity (E1 = 8.25), Improved communication (E2 = 7.4), Increased accessibility (E3 = 7.5), Environmental efficiency (E4 = 7.6) are high, which indicates the high efficiency of electronic document management for the state and individual organisations. However, the high score of Inertia of regulation (E7 = 8.5), as well as the values of the criteria Complexity of legal regulation (E5 = 7.7) and Insufficient data protection (E6 = 7.8), indicate the need to supplement and improve the legal regulation of electronic document management in the global environment (Figure 3).

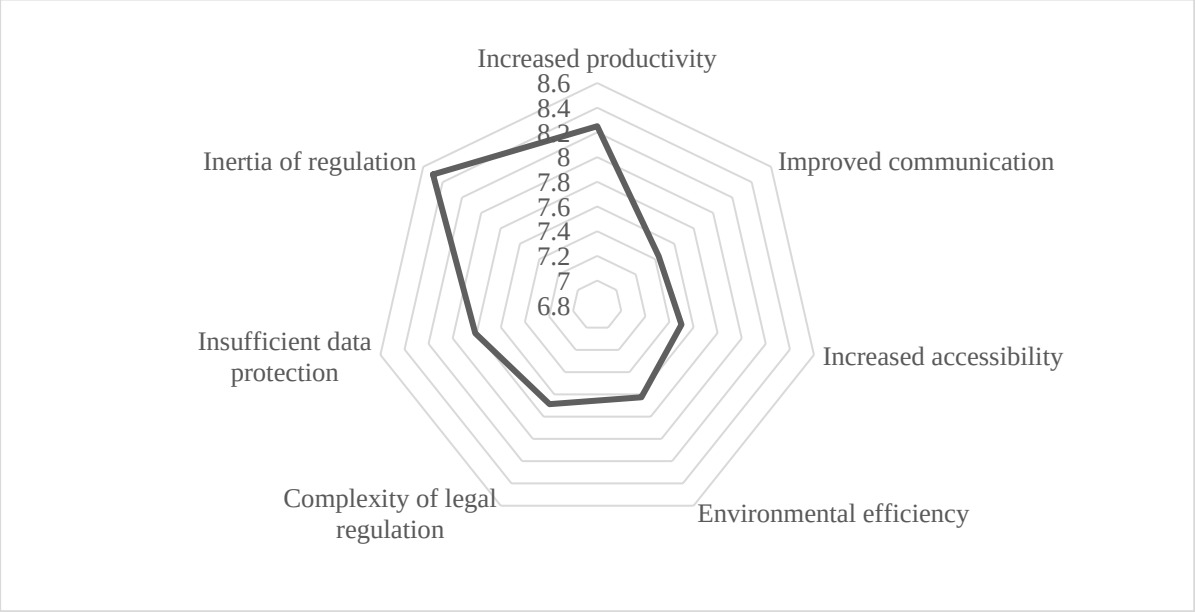

Figure 3: Results of Evaluating the Efficiency Factors of Electronic Document Management
Source: compiled by the author

Experts also assessed technological and organisational measures to avoid and eliminate cybersecurity risks (Appendix B). Thus, the highest weighted average scores were given to Confidential information leakage (K1 = 8.2) and Loss of data (K3 = 7.4), which indicates the need to develop data management mechanisms and precise requirements for data storage (Figure 4).

The results of the correlation analysis of the expert opinions were conducted using Pearson's Correlations tool of the JASP statistical software (Appendix C) and are presented in Table 1.
According to the results of the correlation analysis, it should be noted that the moderate negative correlation between Loss of data and Increased productivity ($r = -0.512$ at $p = 0.043$) indicates that with the increase in the risk of data loss due to a cyber-attack, the productivity of basic operations (including the processes of searching, editing, storing and sharing digital

ISSN: 2408-7920

African Journal of Applied Research
Vol. 11, No. 1 (2025), pp. 173-193
http://www.ajaronline.com
https://doi.org/10.26437/ajar.v11i1.
Received: August 25, 2024
Peer reviewed: October 30, 2024
Revised: December 12, 2024
Published: January 2025

documents) tends to decrease. A similar result was obtained by calculating the correlation between Ineffective cybersecurity measures and Insufficient data protection (r = -0.419 at p = 0.106), indicating that the data protection problem is becoming more acute due to the ineffectiveness of existing cybersecurity measures.

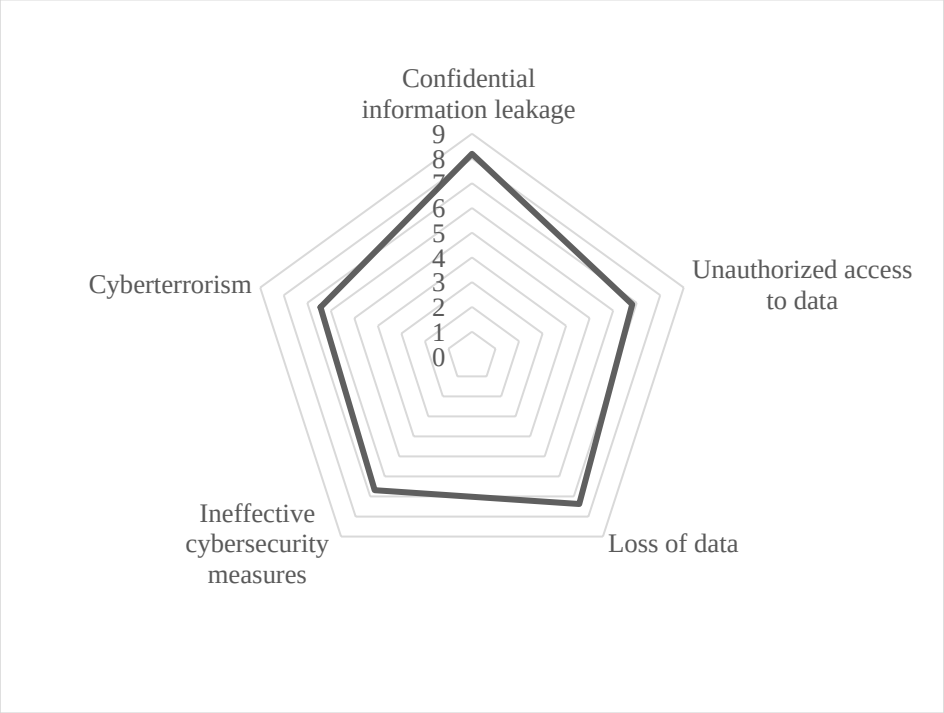

Figure 4: Results of Assessing Cybersecurity Significance Factors
Source: compiled by the author

Table 1: Correlation Analysis of the Impact of Digital Innovations in the Electronic Document Management System on the Level of Cybersecurity

Variable		E1	E2	E3	E4	E5	E6	E7
K1	Pearson's r	-0.141	-0.231	0.336	-0.074	0.113	0.216	0.089
	p-value	0.602	0.390	0.203	0.786	0.677	0.421	0.742
K2	Pearson's r	0.145	0.028	-0.010	-0.030	-0.146	-0.205	-0.118
	p-value	0.591	0.919	0.969	0.913	0.591	0.446	0.663
K3	Pearson's r	**-0.512**	0.195	0.222	0.091	0.021	**0.320**	0.000
	p-value	0.043	0.470	0.408	0.736	0.938	0.227	1.000
K4	Pearson's r	0.388	0.016	-0.380	0.106	0.106	**-0.419**	-0.113
	p-value	0.138	0.952	0.147	0.695	0.697	0.106	0.678
K5	Pearson's r	0.081	0.033	**0.418**	-0.030	0.052	0.033	-0.118
	p-value	0.766	0.903	0.107	0.914	0.847	0.902	0.664

Source: compiled by the author

ISSN: 2408-7920

African Journal of Applied Research
Vol. 11, No. 1 (2025), pp. 173-193
http://www.ajaronline.com
https://doi.org/10.26437/ajar.v11i1.
Received: August 25, 2024
Peer reviewed: October 30, 2024
Revised: December 12, 2024
Published: January 2025

At the same time, the correlation between the criteria Cyberterrorism and Increased accessibility (r = 0.418 at p = 0.107) indicates that increasing data accessibility leads to an increase in the risk of cyberterrorism. However, it improves interaction with users (at the state level - with citizens of the country) and ensures the inclusiveness of information systems. In addition, the positive correlation between the criteria Loss of data and Insufficient data protection (r = 0.320 at p = 0.227) suggests that the increased risk of losing personal and confidential data in electronic documents is due to their insufficient protection.

CONCLUSION

Based on the analysis of the international practice of state interaction with the electronic document management system, the optimal system of legal regulation of such document management should be based on a clear and harmonious legislative framework, covering all aspects of creation, transfer, storage and protection of electronic documents. Given the international experience of states in dealing with digital innovations, the process of comprehensive state coverage of electronic documents is still incomplete. It, therefore, requires the introduction of regulations that will guarantee the legal force of electronic signatures, ensure the security of personal data and establish reliable cybersecurity standards. It should be noted that this goal can be achieved primarily through a combination of international and national legislation and the creation of favourable conditions for cross-border document exchange in the context of expanding globalisation and digital transformation.

The analysis of the positive and negative aspects of the introduction of electronic document management indicates that there are significant prospects for its development, namely, increased productivity by optimising the processes of storing and exchanging digital documents, improving communication between stakeholders, reducing the environmental burden by eliminating the need for resources to create paper documents, ensuring the availability of electronic versions of documents for automated processing and providing the ability to store large volumes of documents.

However, the identified opportunities are complicated by insufficient protection of confidential data, lack of legal instruments to minimise cyber risks, inertia of legal regulation and lack of digital sovereignty. The study showed that electronic document management would increase productivity through automation, which is complicated by the risk of data loss (r = -0.512 at r = 0.043), as well as increase the availability of electronic systems, but at the same time, increases the risk of cyber terrorism (r = 0.418 at r = 0.107). Overall, the study results indicate the need to improve regulatory and security mechanisms to ensure the long-term effectiveness of electronic document management.

ISSN: 2408-7920

African Journal of Applied Research
Vol. 11, No. 1 (2025), pp. 173-193
http://www.ajaronline.com
https://doi.org/10.26437/ajar.v11i1.
Received: August 25, 2024
Peer reviewed: October 30, 2024
Revised: December 12, 2024
Published: January 2025

The research findings have significant practical implications for various stakeholders. Public authorities can use the proposed strategies to improve administrative efficiency and transparency by implementing secure electronic document management systems, thereby reducing operational costs and improving the delivery of public services. The research also has significant social implications, including promoting digital inclusion and accessibility by streamlining digital processes, which expands access to services for different population groups and improves social equity. The emphasis on paperless solutions also aligns with environmental sustainability objectives, as it minimises the environmental harm associated with producing, storing, and distributing paper documents.

REFERENCES

Abacı, K., & Medeni, I. T. (2022). Efficiency of electronic document management systems: a case study. *Science, Education and Innovations in the context of modern problems*, *5*(3), 75–86. https://doi.org/10.56334/sei/5.3.7

Abidin, S. S. Z., & Husin, M. H. (2018). Improving accessibility and security on document management system: A Malaysian case study. *Applied Computing and Informatics*, *16*(1/2), 137–154. https://doi.org/10.1016/j.aci.2018.04.002

Asogwa, B. E. (2013). E-government as a paradigm shift for efficient public services: Opportunities and challenges for Nigerian government. *Library Hi Tech*, *31*(1), 141–159. https://doi.org/10.1108/07378831311303985

Benmakhlouf, H., & Chouaou, A. (2024). Electronic document, information, and archive management systems in economic institutions: A descriptive study of the onbase system. *International Journal of Professional Business Review*, *9*(6), e4755. https://doi.org/10.26668/businessreview/2024.v9i6.4755

Bielialov, T., Kalina, I., Goi, V., Kravchenko, O., & Shyshpanova, N. (2023). Global experience of digitalisation of economic processes in the context of transformation. *Journal of Law and Sustainable Development*, *11*(3), e0814. https://doi.org/10.26668/businessreview/2023.v8i6.2041

Boiko, O. (2024). Electronic Document: Domestic and International Experience of Information Storage. *Bulletin of the KhDAK*, *65*, 25–36. https://doi.org/10.31516/2410-5333.065.02

Bondarenko, S., Makeieva, O., Usachenko, O. Veklych, V., Arifkhodzhaieva, T., & Lernyk, S. (2022). The Legal Mechanisms for Information Security in the Context of Digitalisation. *Journal of Information Technology Management, 14*, 25–58. https://doi.org/10.22059/jitm.2022.88868

Cámara de Diputados (2012). The Law of Advanced Electronic Signature. *Cámara de Diputados*. https://www.diputados.gob.mx/LeyesBiblio/ref/lfea.htm

Check Point Research (2024). Check Point Research Reports Highest Increase of Global Cyber Attacks seen in last two years – a 30% Increase in Q2 2024 Global Cyber Attacks. *Check Point*. https://blog.checkpoint.com/research/check-point-research-reports-

African Journal of Applied Research
Vol. 11, No. 1 (2025), pp. 173-193
http://www.ajaronline.com
https://doi.org/10.26437/ajar.v11i1.
Received: August 25, 2024
Peer reviewed: October 30, 2024
Revised: December 12, 2024
Published: January 2025

highest-increase-of-global-cyber-attacks-seen-in-last-two-years-a-30-increase-in-q2-2024-global-cyber-attacks/

Di Marzo Serugendo, G., Cappelli, M. A., Falquet, G., Métral, C., Wade, A., Ghadfi, S., & Cutting, G. (2024). Streamlining Tax and Administrative Document Management with AI-Powered Intelligent Document Management System. *Information*, *15*(8), 461–494. https://doi.org/10.3390/info15080461

FDIC (2014). Electronic Signatures in Global and National Commerce Act (E-Sign Act). *Federal Deposit Insurance Corporation*. https://www.fdic.gov/system/files/2024-06/x-3-1.pdf

Global Growth Insights (2024). Electronic Document Management System Market Size (USD 7513.54 M) by 2032, by type (Powder, Liquid), by applications covered (Medicine, Functional Foods) and Regional Forecast to 2032. *Global Growth Insights*. (pp. 1–100). https://www.globalgrowthinsights.com/market-reports/electronic-document-management-system-market-101265

Government of Canada (2000). Personal Information Protection and Electronic Documents Act (PIPEDA). *Justice Laws Website Canada*. https://laws-lois.justice.gc.ca/eng/acts/P-8.6/FullText.html

Gruzd, M. V., & Yermolenko, O. O. (2023). Analysis of effectiveness of electronic governance of administrative services provision system. Current issues in modern science, *3*(9), 142–182. https://doi.org/10.52058/2786-6300-2023-3(9)-142-182

Kouroubali, A., & Katehakis, D. G. (2019). The new European interoperability framework as a facilitator of digital transformation for citizen empowerment. *Journal of Biomedical Informatics*, *94*, 103166. https://doi.org/10.1016/j.jbi.2019.103166

Krasnykov, Y., Bobos, O., Lavrinets, I., Khabarova, T., & Zozulia, N. (2024). The Impact of Electronic Governance on the Quality of Public Services and Municipal Property Management. *Pakistan Journal of Criminology*, *16*(1), 201–216. https://doi.org/10.62271/pjc.16.1.201.216

Krysovatyy, A., Desyatnyuk, O., & Ptashchenko, O. (2024). Digital Innovations and their Ramifications for Financial and State Security. African Journal of Applied Research, 10(1), 431-441.

Kussainova, A. K., Hoffmann, T., & Omarova, A. B. (2020). Specifics of international legal and national regulation of electronic document management. *Journal of actual problems of jurisprudence*, *93*(1), 195–208. https://doi.org/10.26577/JAPJ.2019.v89.i1.019

Lovdata (2003). Act relating to electronic communications. *Ministry of Digitalisation and Public Governance*. https://lovdata.no/dokument/NLE/lov/2003-07-04-83#:~:text=The%20Act%20applies%20to%20activity,names%20and%20addresses%20are%20included

Lovdata (2018). Act on the implementation of the EU regulation on electronic identification and trust services for electronic transactions in the internal market (Act on electronic trust services). *Ministry of Digitisation and Administration*. https://lovdata.no/dokument/NL/lov/2018-06-15-44

ISSN: 2408-7920

African Journal of Applied Research
Vol. 11, No. 1 (2025), pp. 173-193
http://www.ajaronline.com
https://doi.org/10.26437/ajar.v11i1.
Received: August 25, 2024
Peer reviewed: October 30, 2024
Revised: December 12, 2024
Published: January 2025

Lovdata (2019). Regulations on trust services for electronic transactions. *Ministry of Digitisation and Administration*. https://lovdata.no/dokument/SF/forskrift/2019-11-21-1577

Nagy, G. (2016). Disruptive developments in document recognition. *Pattern Recognition Letters*, *79*, 106–112. https://doi.org/10.1016/j.patrec.2015.11.024

NetFreedom (2024). Ukraine entered the list of the most attacked countries in cyberspace. *Internet Freedom UA*. https://netfreedom.org.ua/article/ukrayina-uvijshla-do-pereliku-najbilsh-atakovanih-v-kiberprostori-krayin-svitu

Orazgaliyeva, S., Satpayeva, Z., Tazhiyeva, S., & Nurseiytova, G. (2023). E-government as a tool to improve the efficiency of public administration: The case of Kazakhstan. *Management*, *21*(2), 578–591. http://doi.org/10.21511/ppm.21(2).2023.53

Ortina, G., Zayats, D., Akimova, L., Akimov, O. & Karpa, M. (2023). Economic Efficiency of Public Administration in the Field of Digital Development. *Economic Affairs (New Delhi*), *68*(3), 1543–1553. https://doi.org/10.46852/0424-2513.3.2023.21

Pappel, I., Butt, S., Pappel, I., & Draheim, D. (2020). On the specific role of electronic document and record management systems in enterprise integration. In Proceedings of the Fifth International Congress on Information and Communication Technology: ICICT 2020. *Springer Singapore*, *2*, 37–51. https://doi.org/10.1007/978-981-15-5859-7_3

Pappel, I., Pappel, I., Tepandi, J., & Draheim, D. (2017). Systematic digital signing in Estonian e-government processes: influencing factors, technologies, change management. *Transactions on Large-Scale Data-and Knowledge-Centred Systems XXXVI: Special Issue on Data and Security Engineering*, *10720*, 31–51. https://doi.org/10.1007/978-3-662-56266-6_2

Pasichnyk, M., Savchuk, H., Strelbytska, S., Tkach, L., Patrytskyi, V., & Palekha, Y. (2024). Technologies for Electronic Document Management in the Enterprise. In: Štarchoň, P., Fedushko, S., Gubíniová, K. (Eds.), *Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies*, *213*, 199–223. Springer. https://doi.org/10.1007/978-3-031-62213-7_10

Petrosyan, A. (2024). Distribution of cyberattacks across worldwide industries in 2023. *Statista*. https://www.statista.com/statistics/1315805/cyber-attacks-top-industries-worldwide/

Poliakov, O. M. (2023). Modern trends in detecting and countering the use of spyware and malware. *Information and Law*, *2*(45), 125–138. https://doi.org/10.37750/2616-6798.2023.2(45).282332

Pritee, Z. T., Anik, M. H., Alam, S. B., Jim, J. R., Kabir, M. M., & Mridha, M. F. (2024). Machine learning and deep learning for user authentication and authorisation in cybersecurity: A state-of-the-art review. *Computers & Security*, *140*, 103747. https://doi.org/10.1016/j.cose.2024.103747

Rawat, D. B., Doku, R., & Garuba, M. (2019). Cybersecurity in the big data era: From securing big data to data-driven security. *IEEE Transactions on Services Computing*, *14*(6), 2055–2072. https://doi.org/10.1109/TSC.2019.2907247

ISSN: 2408-7920

African Journal of Applied Research
Vol. 11, No. 1 (2025), pp. 173-193
http://www.ajaronline.com
https://doi.org/10.26437/ajar.v11i1.
Received: August 25, 2024
Peer reviewed: October 30, 2024
Revised: December 12, 2024
Published: January 2025

Riigikogu (2000). Digital Signatures Act. *Eesti Riigikantselei*. https://www.riigiteataja.ee/en/compare_original/530102013080

Riigikogu (2001). Law of Obligations Act. *Eesti Riigikantselei*. https://www.riigiteataja.ee/en/eli/506112013011/consolide

Riigikogu (2018). Personal Data Protection Act. *Eesti Riigikantselei*. https://www.riigiteataja.ee/akt/104012019011

Rüßmann, M., Lorenz, M., Gerbert, P., Waldner, M., Justus, J., Engel, P., & Harnisch, M. (2015). Industry 4.0: The future of productivity and growth in manufacturing industries. *Boston Consulting Group*, *9*(1), 54–89. https://inovasyon.org/images/Haberler/bcgperspectives_Industry40_2015.pdf

Shvets, D. V. (2019). Mechanisms for ensuring cyber security in the information space. *Combating cyber threats and human trafficking.* (pp. 14–17). KhNUVS. http://surl.li/zyvzua

Singapore Statutes Online (2010). Electronic Transactions Act. Attorney-General's Chambers of Singapore. https://sso.agc.gov.sg/Act/ETA2010

Singapore Statutes Online (2012). Personal Data Protection Act. Attorney-General's Chambers of Singapore. https://sso.agc.gov.sg/Act/PDPA2012

Stouffer, C. (2022). 115 cybersecurity statistics + trends to know in 2024. *Norton*. https://us.norton.com/blog/emerging-threats/cybersecurity-statistics

Straits Research (2024). Industry 4.0 Market Size & Share, Growth Analysis and Forecast to 2031. *Straits Research*. https://straitsresearch.com/report/industry-4-0-market#:~:text=Market%20Overview,period%20(2023%2D2031)

VRU (2003). On electronic documents and electronic document flow: Law of Ukraine No. 851-IV of 31 December 2023. Legislation of Ukraine. https://zakon.rada.gov.ua/laws/show/851-15#Text

VRU (2017). On electronic digital signature: Law of Ukraine No. 852-IV of 07.11.2018. Legislation of Ukraine. https://zakon.rada.gov.ua/laws/show/852-15#Text

Warner, K. S., & Wäger, M. (2019). Building dynamic capabilities for digital transformation: An ongoing process of strategic renewal. *Long Range Planning*, *52*(3), 326–349. https://doi.org/10.1016/j.lrp.2018.12.001

Zhang, F., Yang, B., & Zhu, L. (2023). Digital technology usage, strategic flexibility, and business model innovation in traditional manufacturing firms: The moderating role of the institutional environment. *Technological Forecasting and Social Change*, *194*, 122726. https://doi.org/10.1016/j.techfore.2023.122726

Zhang, M., & Kaur, M. (2024). Towards a theory of e-government: Challenges and opportunities, a literature review. *Journal of Infrastructure, Policy and Development*, *8*(10), 7707. https://doi.org/10.24294/jipd.v8i10.7707

ISSN: 2408-7920

African Journal of Applied Research
Vol. 11, No. 1 (2025), pp. 173-193
http://www.ajaronline.com
https://doi.org/10.26437/ajar.v11i1.
Received: August 25, 2024
Peer reviewed: October 30, 2024
Revised: December 12, 2024
Published: January 2025

Appendix A

Criteria	Increased productivity	Improved communication	Increased accessibility	Environmental efficiency	Complexity of legal regulation	Insufficient data protection	Inertia of regulation
	E1	E2	E3	E4	E5	E6	E7
Group 1	9	8	8	8	9	10	10
	8	7	9	9	8	8	8
	9	6	7	6	7	10	10
	10	5	9	9	9	9	9
	9	8	6	7	8	10	10
	8	10	8	6	10	7	9
	6	7	9	5	6	9	7
	5	10	10	10	10	3	8
	10	8	8	8	7	10	10
	7	9	10	9	6	9	9
Group 2	9	3	6	4	5	8	6
	7	4	3	9	8	10	8
	10	10	6	8	7	9	10
	8	8	4	7	6	5	9
	8	9	10	8	9	5	4
	9	7	7	9	8	3	9

Appendix B

Criteria	Confidential information leakage	Unauthorised access to data	Loss of data	Ineffective cybersecurity measures	Cyberterrorism
	K1	K2	K3	K4	K5
Group 1	10	9	10	6	6
	9	8	9	9	9
	9	6	6	4	9
	10	6	5	6	8
	6	8	7	5	7
	10	5	8	8	5
	9	7	10	3	5
	8	5	7	5	8
	6	4	8	6	7
	10	7	10	3	6
Group 2	9	7	5	8	7
	8	5	9	7	3
	7	7	5	10	5
	6	8	7	9	7

ISSN: 2408-7920

African Journal of Applied Research
Vol. 11, No. 1 (2025), pp. 173-193
http://www.ajaronline.com
https://doi.org/10.26437/ajar.v11i1.
Received: August 25, 2024
Peer reviewed: October 30, 2024
Revised: December 12, 2024
Published: January 2025

	6	8	7	8	8
	8	9	5	10	3

ISSN: 2408-7920

African Journal of Applied Research
Vol. 11, No. 1 (2025), pp. 173-193
http://www.ajaronline.com
https://doi.org/10.26437/ajar.v11i1.
Received: August 25, 2024
Peer reviewed: October 30, 2024
Revised: December 12, 2024
Published: January 2025

Appendix C

Correlation

Pearson's Correlations

Variable		E1	E2	E3	E4	E5	E6	E7	K1	K2	K3	K4	K5
1. E1	Pearson's r	—											
	p-value	—											
2. E2	Pearson's r	−0.194	—										
	p-value	0.473	—										
3. E3	Pearson's r	−0.243	0.417	—									
	p-value	0.364	0.108	—									
4. E4	Pearson's r	−0.125	0.298	0.229	—								
	p-value	0.644	0.263	0.394	—								
5. E5	Pearson's r	−0.116	0.387	0.330	0.512	—							
	p-value	0.668	0.138	0.212	0.043	—							
6. E6	Pearson's r	0.369	−0.316	−0.186	−0.260	−0.287	—						
	p-value	0.160	0.233	0.491	0.332	0.282	—						
7. E7	Pearson's r	0.388	0.200	−0.247	0.191	0.040	0.377	—					
	p-value	0.138	0.459	0.357	0.478	0.883	0.150	—					
8. K1	Pearson's r	−0.141	−0.231	0.336	−0.074	0.113	0.216	0.089	—				
	p-value	0.602	0.390	0.203	0.786	0.677	0.421	0.742	—				
9. K2	Pearson's r	0.145	0.028	−0.010	−0.030	−0.146	−0.205	−0.118	−0.041	—			
	p-value	0.591	0.919	0.969	0.913	0.591	0.446	0.663	0.881	—			
10. K3	Pearson's r	−0.512	0.195	0.222	0.091	0.021	0.320	0.000	0.250	−0.021	—		
	p-value	0.043	0.470	0.408	0.736	0.938	0.227	1.000	0.350	0.939	—		
11. K4	Pearson's r	0.388	0.016	−0.380	0.106	0.106	−0.419	−0.113	−0.299	0.288	−0.470	—	
	p-value	0.138	0.952	0.147	0.695	0.697	0.106	0.678	0.261	0.279	0.066	—	
12. K5	Pearson's r	0.081	0.033	0.418	−0.030	0.052	0.033	−0.118	−0.053	−0.040	−0.128	−0.215	—
	p-value	0.766	0.903	0.107	0.914	0.847	0.902	0.664	0.845	0.883	0.637	0.424	—

ISSN: 2408-7920