DOI: 10.55643/fcaptp.4.57.2024.4444

Valentyn Biliavskyi
Candidate of Economy Sciences, Associate Professor of the Department of Management of Foreign Economic Activity of Enterprises, National Aviation University, Kyiv, Ukraine;
ORCID: 0000-0003-2129-1524

Yuliia Biliavska
Candidate of Economy Sciences, Associate Professor of the Department of Management, State University of Trade and Economics, Kyiv, Ukraine;
e-mail: y.biliavska@knute.edu.ua
ORCID: 0000-0002-8183-4036
(Corresponding author)

Yurii Umantsiv
D.Sc. in Economics, Professor, Head of the Department of Economics and Competitive Policy, State University of Trade and Economics, Kyiv, Ukraine;
ORCID: 0000-0003-0788-7110

Yaroslav Shestack
Director of the Information and Computing Center of the Main Center of Information Technologies, State University of Trade and Economics, Kyiv, Ukraine;
ORCID: 0000-0002-5102-9642

Oleksandr Zhurba
Candidate of Economy Sciences, Senior Lecturer of the Department of Economics and Competition Policy, State University of Trade and Economics, Kyiv, Ukraine;
ORCID: 0009-0008-3007-4314

Artem Khavanov
Candidate of Economy Sciences, Anti-corruption Commissioner, JSK "The State Export-Import Bank of Ukraine", Kyiv, Ukraine;
ORCID: 0009-0002-9755-3420

Received: 24/05/2024
Accepted: 06/08/2024
Published: 31/08/2024

DIGITAL TECHNOLOGIES IN THE FINANCIAL SECTOR OF THE ECONOMY

ABSTRACT

The article is devoted to the study of the main trends in the development of digital technologies in the financial sector of the economy, namely, the topic is relevant in the context of rapid globalization, digitalization and transition to digital ecosystems. The modern financial sector of the economy at different stages of its life cycle cannot function without the use of digital technologies. In addition, online activity, browsing social networks, and web pages, and using various applications are essential for civil society. The purpose of this paper is to study the changing impact of advanced technologies on digital security, as well as to substantiate the trends in the development of digital technologies in the financial sector of the economy.

The article characterizes the risks arising from the digitalization of the economy - the results of the analysis show that the effective use of these factors can stimulate the competitiveness of financial institutions. The level of threat in data management is investigated, which should be taken into account when forecasting potential threats of digitalization in the financial sector of the economy, which allows the management of institutions to optimize: financial, human and technological resources for risk management and take measures to offset possible losses from cyber threats and restore the stable development of economic systems.

The article identifies trends in the development of digital technologies in the financial sector of the economy that require detailed study and provide for the transition to a modern digital financial platform. This transition will not only strengthen the country's domestic market, increasing the level of independence from the import of foreign technologies but will also contribute to improving the global importance of the economy. Therefore, the use of digital technologies in the financial sector of the economy is of key importance, and effective financing in the new economic reality largely ensures the success of the country's socio-economic development.

Keywords: digital detox, data security, digitalisation, vision, management, finance, economy

JEL Classification: M20, M21, M59, C80

INTRODUCTION

During the COVID-19 pandemic and martial law, the country has undergone fundamental changes in the process of digitalisation. Increasingly, in the world practice, digitalisation indices are calculated and ranked, including the following indices: digital economy (BCG, e-Intensity), digital evolution (DEI), digital economy and society (DESI), world digital competitiveness (WDCI), and global cybersecurity index (GCI). Digital transformation in any country can contribute to capitalisation, prosperity and improved well-being of civil society. By supporting this transformation, governments recognise that digital security and the development of digital technologies should be an integral part of technological progress. The globalisation of economic processes is becoming an important component of the development of modern civil society. The financial sector is the backbone of the country's socio-economic development. The success of the state socio-economic policy, whose main objective is to ensure economic growth and improve the quality of life of the population, depends on how financial resources are generated, distributed and used, and how effective the mechanism of financing the real sector of the economy, science, education and culture is.

Digitalisation is a general trend in modern economic development that covers all areas of both economic and social life. The industry is actively developing and implementing Industry 4.0 technologies, while consumers cannot imagine their daily lives without the Internet, and online meetings and training using Zoom, Skype and Google Meet platforms have become popular. Digital technologies have also affected the financial sector of the economy. Thus, banks are actively using innovative technologies to interact with consumers, and consumers themselves are creating demand for innovative financial products, such as crowdfunding or crowdfunding.

It is worth noting that the key problem is that with the development of digital technologies, new opportunities are emerging for attackers who actively use network scanning attempts, application layer network attacks, DDoS attacks, Web attacks, malware distribution, and phishing. Such threats arise in all countries of the world, and therefore the problem of data security is becoming more relevant and important, especially under the influence of rapid globalisation changes, which is important to foresee in the trends of digital technologies. Cyber threats and various types of cyber fraud are rightly considered to be a particularly dangerous risk, but financial security institutions are also strengthening their defences using new digital tools. In the process of digitalising the economy, social risks associated with job losses are also significant. However, not only new financial services, banking products, and new digital innovation programmes are being offered, but also new types of employment in the financial sector are emerging, and the education sector is developing the most effective systems for training financial institution staff, taking into account their specifics.

LITERATURE REVIEW

The theoretical, methodological and practical aspects of diagnostics and digital technologies' agendas are described in the works of some domestic and foreign researchers. In particular, Mariano et al. (2021) addresses the issue of digital technologies as a concept that determines the development of socio-economic systems under the dominant influence of information and technology. The presented system is based on behavioural determinants that take into account: behavioural, cultural and social components. Also, organisational or social changes based on the implementation of digital technologies are presented in Remeikiene et al. (2021), where the authors are convinced that digital transformation is a change in human nature, thinking, living and governance that has been shaped by digital technologies. Such studies take into account the impact and features of digital technologies in any sector of the country's economy and do not focus directly on financial subsystems.

Yerina et al. (2021) argue that cybersecurity ratings play the role of a kind of identifier of the relative strengths and vulnerabilities of national cyber strategies, and also point to the need to revise them to strengthen protection against cyber-attacks and improve cyber risk management. The authors prove that countries with a high level of economic development based on the contribution of IT technologies to national production have a higher digital security potential, regardless of geolocation. The authors' correlation between the Global Cybersecurity Index (GCI), indices of information society development (IDI, NRI, EGDI) and GDP per capita confirms that the digital transformation of civil society and the economy in a country is a key driver of economic development only if information and cybersecurity are ensured. Bondarenko et al. (2022) consider a group of indices that can be used to measure information security, namely: the index of information computer technology development, the global cybersecurity index, the network readiness index, the national cybersecurity index, and the level of digital development of the country. Taking into account the described indices, the authors propose to calculate the index of digital capability and cybersecurity of a country.

Digital technologies as key tools for mitigating and counteracting the most pressing environmental and social problems of our time are a current research trend in science (Dwivedi et al., 2022; Papagiannidis & Marikyan, 2022). This view is also confirmed by the sharp increase in the number of digital sustainable patents and the increase in venture capital investment (Anderson & Caimi, 2022). Shestack et al. (2023) describe that the issue of digital competencies and descriptors is becoming particularly relevant in the digital sector.

Scientific interest in digitalisation technologies is represented by research related to: the introduction of legal protection in the economy, finance and blockchain management, artificial intelligence, cryptography, cloud technologies, and knowledge management. Digital technologies, such as platforms, blockchain, artificial intelligence (AI), virtual reality (VR), or the Internet of Things (IoT), have transformed numerous industries (housing, agriculture, and transport), providing enterprises with unprecedented advantages and new business opportunities (Nambisan, 2017; F. von Briel et al., 2018). It should be noted that any industry needs financial support, and the results of their activities are the direct development of the financial sector of the country's economy.

DOI: 10.55643/fcaptp.4.57.2024.4444

Scientometric databases contain a significant number of publications on a particular topic (Onopriienko et al., 2023). For example, the Scopus scientometric database contains more than 825 thousand papers on the keyword «digital technology». Summarising the information obtained, Figure 1 shows a network visualisation of the term «digital technology».

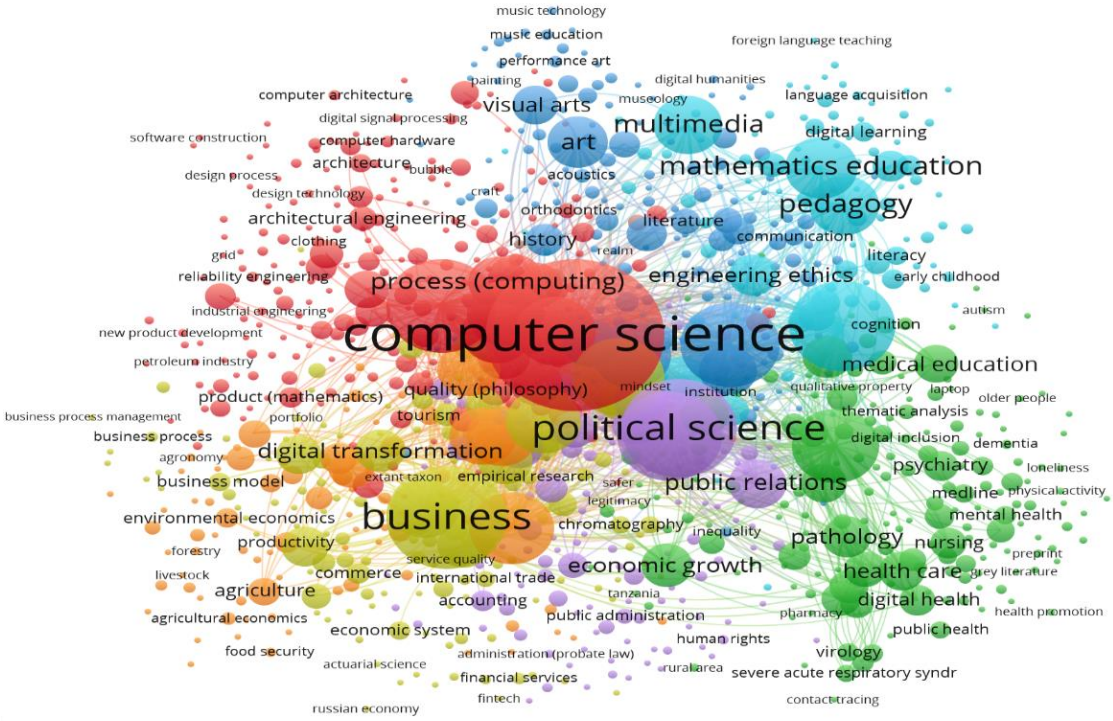

Figure 1. Network visualisation of the term «digital technology». *(Source: created by the authors using VOSviwer software based on the Scopus database)*

The results allow us to conclude that publications on digital technologies not only remain in trend but also develop in different scientific areas. The data analysis has identified eight clusters where the term «digital technology» is interrelated. For example, the red cluster shows the interconnection of publications focused on: computer science, computer architecture, manufacturing engineering, ecosystems, and workflow. The green cluster indicates that digital technologies are described in scientific papers on medicine, psychology and healthy lifestyles. The interrelationships of papers in the blue cluster are publications that present digital technologies from a scientific point of view (management, mathematics, and educational projects). In the purple cluster, the connection of digital technologies with public administration, political systems, and data protection at the state level can be traced. A separate cluster focuses on information support (information security, services, data storage, cloud technologies), and another on business and management processes, business models, and economic systems.

There is also a cluster that highlights digital technologies in ecology, agriculture, food and other industries. There is a separate cluster in which keywords indicate the development and vision of digital technologies for the future or transformation processes and the transition to artificial intelligence. However, each of these clusters requires financial support and financial transactions. As a result of data filtering, it was found that the Scopus scientometric database contains 9086 papers on digital technologies in the financial sector. For example, Daud et al. (2024) examine the impact of financial inclusion and digital technologies on economic growth. The authors prove that digital technologies improve financial inclusion in general and eliminate the gender gap in financial inclusion, as well as complement the impact of financial inclusion on economic growth. However, there is no mention of possible risks in digital technologies in such conditions of the financial sector of the economy.

An interesting study is by Bas et al. (2024), and Prokopenko et al. (2023), in which the authors focus on the relationship between central bank digital currency index, financial stability, and digital assets. NFTs show a moderate relationship, a distinct segment within the broader asset universe, and there is a bi-directional relationship between CBDCs and financial stability indicators. A different perspective on digital technologies in the financial sector is presented by Saud et al. (2024), who examine the cultural dynamics of the digital space. It should be noted that the study is highly specialised,

and the proposals are aimed exclusively at young people, who are better oriented in virtual spheres than other generations.

The digital transformation of the financial sector in the context of the COVID-19 pandemic is also worth mentioning (Battisti et al., 2022; Zaban & Plaut, 2024). The difference between such works is that the presented studies and trends are focused exclusively on the working conditions in force majeure situations, such as a «pandemic» or «war». Ghosh (2024) summarises the work by conducting a bibliometric analysis of research on financial inclusion and designing a sustainable future. A common word analysis analysed key themes from the research to better understand the field. This allowed us to demonstrate a clear future direction in research on digital trends in the financial sector.

The key hypothesis of the study is that the rapid transition to total digital transformation has both positive and negative consequences in the financial sector of the economy. Civil society is not ready to give up the conveniences provided by high technology but underestimates the potential threats associated with data security.

AIMS AND OBJECTIVES

The purpose of the article is to study the changing impact of advanced technologies on digital security, as well as to substantiate the trends in the development of digital technologies in the financial sector of the economy.

To achieve this goal, the following objectives have been formed:

- to characterise the risks arising from the digitalisation of the economy;
- to investigate the level of threat in data management in the financial sector of the economy;
- to identify trends in the development of digital technologies in the financial sector of the economy.

METHODS

The scientific, theoretical and methodological basis for the implementation of the defined tasks is the work of domestic and foreign scholars in the field of digital technologies. In the process of working on the article, special and general scientific research methods, as well as data processing software, were used. The abstract and logical method allowed clarifying the categories of digital technologies in the financial sector of the economy and specific terms; the analysis and synthesis method allowed substantiating the conceptual provisions of the process of managing risks arising from the digitalisation of the economy; the systemic and structural method helped structuring the levels of threats in data management; the graphical method was used to summarise the trends in the development of digital technologies in the financial sector of the economy in the form of K. Ishikawa's diagram.

For the bibliometric analysis, the author used data from scientific publications published in the Scopus scientometric database and processed using the VOSviewer software. The use of the software made it possible to identify the main links between the existing data visualisation concepts.

RESULTS

The organisation of financial data security management at the national level is a matter of choice for each country and largely depends on legal support and regulation at the state level. Factors such as the availability of data security experts, financial support, and national and strategic plans for economic and internal security influence the formation of an effective digital security system.

Given the high dynamics of the implementation of digital technologies in traditional sectors, as well as the formation of new digital segments, an intensive transformation is underway: technological, managerial and business approaches in the modern economy. In this context, the risks associated not only with the stable development of macro- and microeconomic systems in the digital ecosystem but also with their vulnerability to growing cyberattacks and threats to national security in the critical infrastructure sector are growing significantly. That is why it seems important to identify the risks associated with the digitalisation of the financial sector of the economy, and classify them by the degree of probability and potential for possible damage, both at the level of the enterprise and the country as a whole (Table 1).

DOI: 10.55643/fcaptp.4.57.2024.4444

Table 1. Characteristics of risks arising from the digitalisation of the financial sector.

Areas	Characteristics	Risks
Electricity dependence and vulnerability	Information on paper was vulnerable to fire, water, and other physical damage. This vulnerability remained for electronic media, and the risks of simultaneous damage to entire databases were added. Especially in the context of missile attacks on infrastructure	▪ Sudden power outages, in the absence of stabilisers, can easily lead to the loss of operational data and damage to stored data. ▪ Even a single computer virus-infected node with sufficient access rights in a local network can compromise the entire enterprise. ▪ Information concentrated on USB sticks and hard drives is usually lost all at once.
Risks Office 365	SharePoint Online, OneDrive, and Microsoft Teams allow you to share data across the enterprise. Over time, Office 365 becomes a set of public links and unlimited access to confidential data. External links provide access to specific users outside the network	▪ Disclosing sensitive data through guest access and public links poses a serious security risk. ▪ Collaboration in Microsoft Teams is chaotic and should be combined with comprehensive access rights monitoring and user behaviour analytics to detect suspicious activity in Office 365. ▪ To prevent password brute-force and credential spoofing attacks, all employees should have multi-factor authentication enabled
DDoS attacks	A distributed denial-of-service attack is an overload of the attacked server with a large number of external requests. It is difficult to defend against this, as such requests do not differ much from those of real users, but are made automatically	▪ Computer resources become inaccessible to targeted users, making interaction impossible and undermining trust in the reliability of the resource owner. ▪ In fact, it is available to many medium-sized competitors and hacker groups of aggressor states, as it requires only control over a large number of Internet nodes
User and device activity	User and device activity includes activities in cloud and on-premises file systems, email and SharePoint, perimeter and Active Directory telemetry, and threat analysis. Applications such as Varonis monitor and analyse the behaviour of users and objects in cloud and on-premises storage, detecting and alerting to insider threats	▪ Unauthorised attempts to access or modify data to data or modify data often indicate insider threats, cyberattacks, or malware activity. ▪ Unusual user or device behaviour may indicate a potential account takeover or data breach. ▪ Connections from inactive users or connections to malicious IP addresses often indicate an active cyberattack: attackers are trying to gain access to an account or system or steal data
Application programming interfaces (APIs)	Modern hardware and software systems consist of a large number of systems that are separate and independent in order to remain modular. At the same time, the number of potential connections between systems is the square of their number - much more, so integrations are often developed by third-party contractors, with less careful consideration of the security features of the systems	▪ Often, the modifications made to the programme during the integration process have unlimited software access to its resources. ▪ In order to optimise and save development time, incoming data is not always thoroughly checked. ▪ In particular, an outdated specification of data types and restrictions can lead to inadmissible values being entered into the system and unpredictable failures in its operation. ▪ Authorisation, authentication, and token validity are also at risk
Software compromise	Software developers have the ability to make hidden, undocumented modifications that work in their favour. Often, this is an attempt to prevent piracy or to make quick fixes, but it all depends on the integrity of each employee of the developer. Sometimes such functions are close to viruses	▪ Backdoors are pre-conceived methods of unauthorised remote access. Even initial passwords that have not been changed by the user and some debugging functions that have not been removed in the final version can act as backdoors. ▪ Functions for collecting statistics, telemetry, logs, dumps, etc. may contain confidential user data in general and their actions in a particular situation
Identity theft, anonymity, social engineering	In the pursuit of ease and speed of service delivery, as well as privacy, Internet service providers, websites, and individual applications are reducing the requirements for personally identifiable information. Artificial intelligence technologies allow us to generate images, voices and actions that are difficult to distinguish from real people. Meanwhile, even the willingness to follow the instructions of 'system administrators' without checking the sender's address remains a problem.	▪ It is not always possible to trace at least the formal owner of the computer from which the hacker attack was launched. ▪ The less personal information a user provides, the easier it is to make statements or actions on their behalf, and the more, the greater the risk of leakage and blackmail. ▪ People are not used to questioning the identity of the person they are texting, talking to, or even seeing via video, and this could be an intruder or a deepfake. ▪ Even without a deep fake, not all employees have sufficient computer competence to distinguish between intruders and avoid performing dangerous actions

It is worth noting that publicly accessible data is a common security vulnerability. According to information security experts, it takes almost 6-8 hours per folder to find and delete global access groups manually, without automation. Experts should identify the users who need access, then create and apply new groups, and only then add the necessary users to them. Sensitive data shared with global groups poses a significant risk to the business. It should be identified and remediated so that only those users who need to know it to perform their job functions have access to it.

The high-tech future empowers civil society and facilitates both positive and negative outcomes in the handling of information and digital data. The rapid development of technology has changed the way we work with data, opening up new opportunities for communication, work and entertainment. But as technology evolves, so do data security threats. Any new technology quickly becomes a threat in cyberspace, with attackers hunting for information, finances, and other resources. Therefore, it is now crucial for digital security professionals to pay attention not only to current threats but also to future threats. In order to study the risks in the financial sector of the economy, Table 2 identifies the levels of impact on the threat in data management.

Table 2. Determining the level of impact on the threat in financial data management.

Level of impact on the threat	Characteristics	Technology rating
A	The technology has a significant impact on the threat landscape, creates opportunities for fundamentally new attacks, creates new attack surfaces or significantly changes existing ones. The impact is also assessed as high if the technology can be used to protect against cyber threats and has a significant advantage over existing protection methods	High
B	Technology impacts the threat landscape, does not enable fundamentally new attacks or defences, but can significantly improve the effectiveness of existing attacks or defences Technology impacts the threat landscape, does not enable fundamentally new attacks or defences, but can significantly improve the effectiveness of existing attacks or defences	Medium
C	The technology has virtually no impact on the threat landscape, nor does it affect the emergence of new threats or defence methods. Provides only a small increase in the effectiveness of attacks or defence methods	Low

The presented levels of impact on the threat are attributed to one of three time periods, depending on when the technology is expected to reach the peak of maturity, which makes it possible to apply it widely in various sectors of the economy (Figure 2).

The impact of changes in digital technologies				
	High	Deep fake, human factor risk management, driverless vehicles, behavioural biometrics, remote work technologies, Bring Your Own Identity (BYOI), digital fingerprint management	Social ranking, artificial intelligence with personal data protection, differential privacy, digital twins, training in artificial intelligence, projection telephony	Powerful artificial intelligence (AGI), quantum computers, global intelligence, artificial intelligence in specific medical areas, population augmentation, bidirectional neurocomputer interface
	Medium	Smart badges, artificial intelligence as a bot, health passport, device identification management, professional video analytics	Generative artificial intelligence, unidirectional neurocomputer interface, neuromorphic microelectronics, multi-cloud	DNA for information storage, DNA gadgets, individualised medicine, digital twins, Internet of Things, decentralised autonomous organisations
	Low	VR/AR, 5G, social distancing and remote work technologies, blockchain	Virtualisation of stores, creation of virtual images, assistants, partners	XR, 3D bioprinting, biodegradable sensors, hyper-personalisation, AI creativity XR, 3D bioprinting, biodegradable sensors, hyper-personalisation, AI creativity
		2024-2025	**2026-2029**	**2030-2032**
		Time period		

Figure 2. Changes in the impact of advanced digital technologies in the financial sector. Note The X-axis in the graph is the time in years, divided into three intervals: up to 3 years, up to 5 years, and more than 7 years. The Y-axis is the impact on the digital landscape, also divided into 3 intervals: low, medium, and high.

According to Figure 2, time periods are defined that have their own peculiarities in terms of digital technology development and management.

1. The vision for the next 3 years includes human factor risk management, as the problem of countering attacks on humans is extremely relevant both for individual enterprises and the cybersecurity industry as a whole. During this period, methods should be developed to assess exposure to various risks, effectively train employees and customers/consumers in threat countermeasures, and develop cyber hygiene skills.
2. The 5-7-year vision envisages the active work of artificial intelligence while maintaining confidentiality. The technologies are directly related to data security, and their research and development will help businesses implement new services related to data access and exchange and training of more accurate and large-scale AI models without creating threats to the privacy and confidentiality of participants.

DOI: 10.55643/fcaptp.4.57.2024.4444

3. The vision for more than 7 years envisages the era of Artificial General Intelligence (AGI), as the emergence of this technology can generate large-scale threats (up to existential ones), both in cybersecurity and beyond. In addition, AGI can significantly affect the cybersecurity industry itself if it is used to protect against threats. Most of the technologies shown in Figure 2 can be classified into one of three categories: artificial intelligence technologies, computing technologies, or technologies for interacting with computing devices. Restrictions related to the COVID-19 pandemic, martial law, process automation, job cuts and structural changes in employment are among the factors that will contribute to the growth of multifunctional specialists.

Thus, as expected, digitalisation and automation are becoming the most important megatrends in the financial sector. Individuals, businesses, and e-governments are consuming more and more internet traffic as digital services such as mobile banking, online shopping, online learning, media, and online communication proliferate. The growth of digital consumption will continue as restrictions caused by demographic, geographic or social factors cease to apply. The healthcare and agriculture sectors are expected to rise.

All of the above processes tend to accelerate in times of force majeure under the influence of globalisation. In particular, systemic 'new wave' technologies, such as 5G, artificial intelligence, augmented and virtual reality, robotics, cloud localisation, geolocation and electronic payment technologies, localisation of entertainment and gaming solutions, and many others. These transformational processes are taking place almost everywhere, even though the 5G rollout has been suspended in some countries due to geopolitical restrictions. Other trends include an increase in demand for: telecommunications, platform and storage technologies. Thanks to communication and Wi-Fi technologies, any smart device can be controlled remotely via the Internet using applications such as Any Desk and Team Viewer. For system integrators, the availability of such a function means new requirements for corporate customers who develop and manage IoT systems. Developing effective mechanisms for forecasting potential threats to the digitalisation of various sectors of the economy is a crucial task that will allow further optimisation of the financial, human and technological resources of the enterprise, country, and integration association for risk management in order to offset possible damage from cyber threats and restore the stable development of economic subsystems. Figure 3 shows a causal diagram of overcoming the risks arising from the digitalisation of the financial sector of the economy.

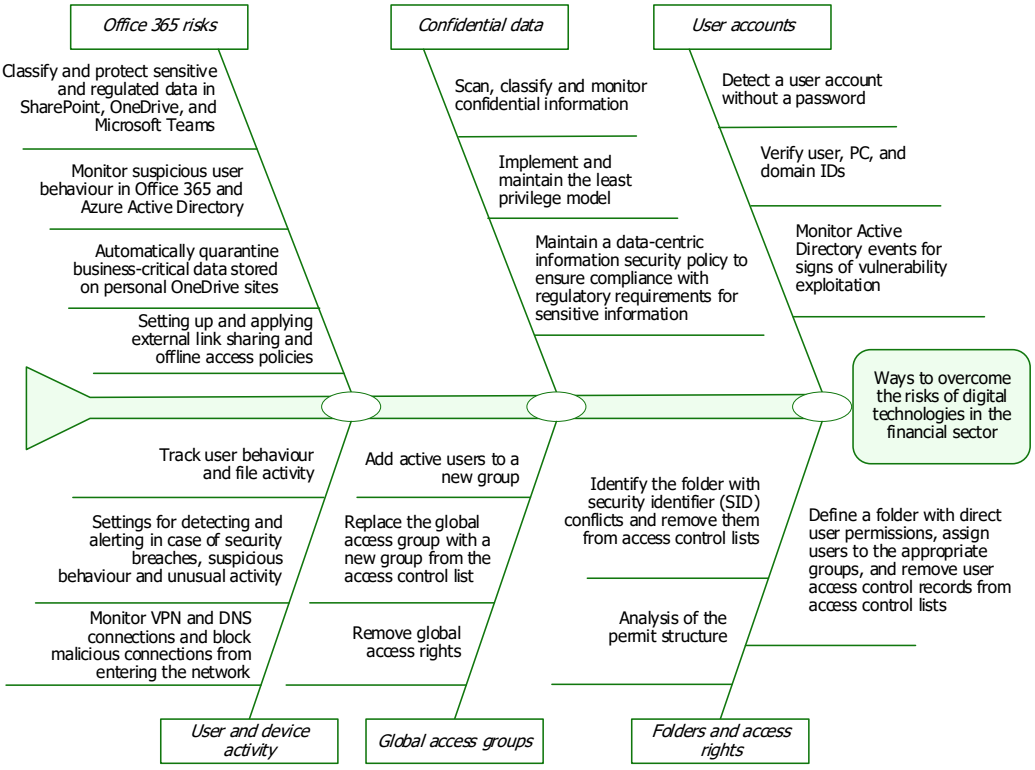

Figure 3. Cause-and-effect diagram of ways to overcome the risks of digital technologies in the financial sector.

As a result of the risk analysis, it can be noted that digital enablers such as the digital workplace; digital engineering and manufacturing; digital supply chain; digital products, services and business models; and digital customer and channel

management allow for the coverage of internal and external processes of the digital ecosystem to satisfy market participants. Despite the numerous advantages, we should not forget about the risks at all levels of the ecosystem, as they pose varying degrees of threat to the enterprise.

That is why the use of any methods, such as the formation of a digital ecosystem risk matrix, will help protect the enterprise and preserve its resource potential (Osiyevskyy, 2023).

Trends in the development of digital technologies lead to the fact that Industry 4.0 is losing its position as a «trend of the future» and is transforming into digital ecosystems for Society 5.0. Modern organisational theories and models are aimed at expanding the capabilities of automation, CRM systems, maximum use of cloud technologies, 3D and VR, as well as various technologies and capabilities, taking into account force majeure circumstances such as a «pandemic» or «war».

The development of entrepreneurial activities through the creation of digital ecosystems creates sustainable and productive operations (Pazaitis et al., 2017). Supported by advanced digital technologies such as artificial intelligence (R. Nishant et al., 2020), this can increase the efficiency and effectiveness of operations by prioritising. Collective intelligence can also help to mitigate and counter the challenges of systemically outdated governance approaches.

The pandemic and various wars (armed conflicts, information wars, trade conflicts, etc.) have significantly accelerated digital transformation and increased demand for information technology around the world. As a result, remote work is becoming the new normal, as expected. Computer-based solutions are essential for the efficient organisation of online work, which is driving the growing demand for cloud platforms. However, it is important to bear in mind that as cloud computing becomes more widely available, the network may not be able to cope with the excessive amount of data uploaded. Increasing data transfer speeds and new media formats are also increasing the demand for data collection systems. The technical power of mobile devices is approaching its limits, which is one of the reasons for the transition to cloud-based technologies. It is worth noting that the communications technology and computer electronics sectors are the most susceptible to geopolitical and pandemic crises. This is why a number of paradoxical scenarios arise for deepening transformation processes. One of the most advanced areas is «cloud democracy», which implies online access to government organisations (for example, open cloud platforms serving citizens on micro-democracy, «digital citizenship» or electronic exchanges for public sector services, etc.) Experts are convinced that digital legislation will become the norm within a decade. Another area is «total digital monitoring», which will become one of the main factors affecting the competencies that are currently in demand in the sector. Wide network coverage, covert video surveillance systems, the proliferation of UAVs and online tracking make our actions, both in the physical and digital world, fully transparent to state and local governments, as well as commercial enterprises.

That is why this study should focus on the following trends in the development of digital technologies in the financial sector of the economy:

- ***Security.*** Data security is of interdisciplinary importance, as it is intended to regulate the work of users with any formats and media and to be listened to by devices and phones. The activities of cyber forensic experts and network detectives who investigate and prevent cybercrime are becoming increasingly important. The key skills in these areas include forensics, investigation, information retrieval and processing. Privacy experts and personal profile security consultants are also in demand, checking and editing information about the user and his or her actions on the Internet and eliminating vulnerabilities.
- ***Network and data storage.*** Key professional roles and skills include network integration architecture (reverse engineering and integration of IT and network processes, ITSM, DevOps), database management, and edge computing development. DevOps / SysOps / NetDevOps combines software development and IT operations and brings teams together to implement joint projects on different platforms. An information systems architect is responsible for: data processing systems, database and algorithm design, quality control, logic, and access to information.
- ***Programming and design.*** Designing software in the field of computer technology requires automated machine learning (AutoML) metaprogramming skills. The design of visual and intuitive interfaces for industrial and commercial applications will be predominantly focused on the development of touch and brain (neural) interfaces. Robotics, 5G networking, and the design of environments saturated with electronic devices are areas where hardware and software come together. Quantum computing is already used in many areas today, and research is a relevant competence in this area. The commercial application of this technology, particularly for analysing and ensuring the safety of complex systems, will continue to grow.

DOI: 10.55643/fcaptp.4.57.2024.4444

- ***Humanisation of technology.*** The development of artificial intelligence technologies and automation leads to the fact that global control over society is concentrated in the hands of a small group of companies, and therefore the profession of a digitalisation coordinator (Digital Regulator) is gaining in importance. The most important competency in this area is knowledge of data ethics.

Thus, the development of the modern world economy, characterised by rapid globalisation processes, has led to the formation of the information society. This leads to changes at the level of civil society (change in social consciousness) and the individual (change in thinking to digital). Following the trends of digital technologies will lead to the growth of digital innovations in the global economic environment.

Of course, digital transformation means the integration of digital technologies into all areas of business, and the continuous renewal of digital potential in the financial sector of the economy requires timely response and adaptation of relevant technological transformations.

Neglecting global changes can lead to a loss of a company's competitive position in the market, and, accordingly, to a deterioration in the country's reputation and a decrease in its rating in various global index rankings. In order to successfully implement your project in the digital transformation era, it is important to gain digital experience by building your own online space. Businesses that have digital innovation platforms and create digital ecosystems can easily become trendsetters in their business areas.

DISCUSSION

The controversial issues in this paper include a number of positions related to the concept of digital technology trends in the financial sector of the economy. Currently, scientific approaches to the study of digitalisation focus on the analysis of blockchain and artificial intelligence. Financial service providers see blockchain technology as useful for improving authenticity, security, and risk management. Blockchain is being used in trading and financial subsystems to create smart contracts between participants, increase efficiency and transparency, and open up new profit opportunities. The unique capabilities of Blockchain are significantly enhancing some of the technological processes in the financial sector. Banks and other financial institutions are using blockchain-enabled identifiers to identify people. The increase in efficiency is due to the ability of businesses to anticipate new trends in financial blockchain applications and develop blockchain functionality. The procedure for transferring ownership of assets and resolving financial issues is simplified (Javaid, M et al., 2022). In turn, Abad-Segura et al. (2024) identify and prove the relevance of factors influencing the safe perception of accounting using blockchain technology. It should be noted that blockchain technology is developing rapidly, but it is still not possible for some countries. Also, there are certain gaps in the legislation of countries and direct permission to use blockchain, AI or VR exclusively in the activities of the enterprise.

The literature review and identification of suspicious information in the financial subsystems of digital business by Pinto et al. (2022) contributed to the development of scientific thought on changes in the impact of promising digital technologies in the financial sector of the economy, which allowed us to summarise them in Figure 2. The study found that scientists have conducted research on digital technologies in the financial sector of the economy in various areas of activity. For example, the development of key performance indicators for monitoring sustainability in the ceramic industry: the role of digitalisation and industry 4.0 technologies described by Contini et al. (2024) and the benefits of digital banking by Saif et al. (2024) allowed us to develop a causal diagram of ways to overcome the risks of digital technologies in the financial sector.

Information technologies play a crucial role in the modern economic system, acting as a driver for the development of the state. Information technologies are not only one of the most important factors stimulating economic growth but also contribute to the development of society, employment stimulation, and competition enhancement (Yankovoi et al., 2023). The development of the database and implementation of methodological approaches is impossible without digital technologies in retail (Biliavska et al., 2024).

We agree with the opinion of Varga et al. (2021), who confirms the existence of cyber threats and risk management in the financial sector of the economy. The paper presents an improvement in risk management practices that aims to ensure the integration of cyber staff into crisis management teams. Ceylan, I.E., & Ceylan, F. (2024) assess research articles on central bank digital currencies (CBDCs) and focus on emerging topics. The analysis identifies bibliometric characteristics of the CBDC literature, including: publication trends, influential countries, influential articles, prolific authors, levels of collaboration, and common keywords. This allows us to formulate prospects and trends in the financial sector of the economy, including data security and information protection.

The limitation of the study presented here is that a bibliometric review of the literature on digital technologies in the financial sector was not fully carried out. This makes it impossible to identify global trends in digitalisation by individual countries, as some of them have significant advantages in digital technologies.

What is different from previous studies is that the trends in the development of digital technologies in the financial sector of the economy are described. They allow not only to assess the current state but also to develop an optimal development plan for the future, taking into account digitalisation tools.

CONCLUSIONS

The paper characterizes the risks arising from the digitalization of the economy, and the results of the analysis show that the effective use of these factors can stimulate the competitiveness of financial institutions. Modern information technology requires innovative approaches to working with graphic materials and programming, the ability to work with video and photo editors, and basic copywriting skills. Data protection policy requires digital communication skills, as it allows the formation and implementation of content plans for social networks: tracking trends, developing algorithms and conducting analytics.

The level of threat in data management, which should be taken into account when forecasting potential threats of digitalization in the financial sector of the economy, is investigated, which allows the management of institutions to optimize: financial, human and technological resources for risk management and take measures to offset possible losses from cyber threats and restore the stable development of economic systems.

The article identifies trends in the development of digital technologies in the financial sector of the economy that require detailed study and provide for the transition to a modern digital financial platform. This transition will not only strengthen the country's domestic market, increasing the level of independence from the import of foreign technologies but will also contribute to improving the global importance of the economy.

Therefore, the use of digital technologies in the financial sector of the economy is of key importance, and effective financing in the new economic reality largely ensures the success of the country's socio-economic development.

Digital transformation in the country's economic sector is necessary because, without the implementation and development of a new technological base for socio-economic processes, it is impossible to ensure economic growth in the country and improve the living standards of the country's population. The use of digital technologies in the financial sector of the economy is of key importance. Effective financing in the new economic reality largely ensures the success of the country's socio-economic development. Thus, the recommendations are to expand the scope of digital technologies in the financial sector of the economy. The transition to a modern digital financial platform will not only strengthen the country's domestic market, increasing the level of independence from the import of foreign technologies but will also help improve the global significance of the economy.

ADDITIONAL INFORMATION

AUTHOR CONTRIBUTIONS

Conceptualization: *Valentyn Biliavskyi, Yuliia Biliavska*
Data curation: *Yuliia Biliavska*
Formal Analysis: *Valentyn Biliavskyi, Oleksandr Zhurba, Artem Khavanov*
Methodology: *Valentyn Biliavskyi, Yuliia Biliavska, Artem Khavanov*
Software: *Yuliia Biliavska, Yaroslav Shestack*
Resources: *Valentyn Biliavskyi, Yurii Umanciv, Artem Khavanov*
Supervision: *Yurii Umanciv, Oleksandr Zhurba*
Validation: *Valentyn Biliavskyi, Yuliia Biliavska, Yurii Umanciv, Oleksandr Zhurba*
Investigation: *Valentyn Biliavskyi, Yurii Umanciv, Yaroslav Shestack, Oleksandr Zhurbai, Artem Khavanov*
Visualization: *Yuliia Biliavska, Yaroslav Shestack*
Writing – review & editing: *Yaroslav Shestack*
Writing – original draft: *Yuliia Biliavska*

DOI: 10.55643/fcaptp.4.57.2024.4444

FUNDING

The Authors received no funding for this research.

CONFLICT OF INTEREST

The Authors declare that there is no conflict of interest.

REFERENCES

1. Abad-Segura, E., Infante-Moro, A., González-Zamar, M.D., & López-Meneses, E. (2024). Influential factors for a secure perception of accounting management with blockchain technology. *Journal of Open Innovation: Technology, Market, and Complexity,* 100264. https://doi.org/10.1016/j.joitmc.2024.100264
2. Anderson, J., & Caimi, G., (2022). A Three-Part Game Plan for Delivering Sustainability Digitally. https://www.bain.com/insights/a-three -part-game-plan-for-delivering-sustainability-digitally/
3. Bas, T., Malki, I., & Sivaprasad, S. (2024). Connectedness between central bank digital currency index, financial stability and digital assets. *Journal of International Financial Markets, Institutions and Money, 92,* 101981. https://doi.org/10.1016/j.intfin.2024.101981
4. Battisti, E., Alfiero, S., & Leonidou, E. (2022). Remote working and digital transformation during the COVID-19 pandemic: Economic–financial impacts and psychological drivers for employees. *Journal of Business Research, 150,* 38-50. https://doi.org/10.1016/j.jbusres.2022.06.010
5. Biliavska, Y., Romat, Y., Biliavskyi, V., Sydorenko, O., & Ostapenko, T. (2024). Diagnosing category management in a pharmacy retail chain. *Eastern-European Journal of Enterprise Technologies*, *1*(13(127), 22–32. https://doi.org/10.15587/1729-4061.2024.298093
6. Bondarenko, S., Makeieva, O., Usachenko, O., Veklych, V., Arifkhodzhaieva, T., & Lernyk, S. (2022). The Legal Mechanisms for Information Security in the context of Digitalization. *Journal of Information Technology Management, 14 (Special Issue: Digitalization of Socio-Economic Processes), 25-58.* https://doi.org/10.22059/jitm.2022.88868
7. Ceylan, I. E., & Ceylan, F. (2024). A bibliometric analysis of global scientific research on central bank digital currencies. *Reference Module in Social Sciences*. https://doi.org/10.1016/B978-0-44-313776-1.00189-6
8. Contini, G., Peruzzini, M., Bulgarelli, S., & Bosi, G. (2023). Developing key performance indicators for monitoring sustainability in the ceramic industry: The role of digitalization and industry 4.0 technologies. *Journal of Cleaner Production, 414,* 137664. https://doi.org/10.1016/j.jclepro.2023.137664
9. Daud, S.N.M., & Trinugroho, I. (2024). Financial inclusion, digital technology, and economic growth: Further evidence. *Research in International Business and Finance*, *70*, 102361. https://doi.org/10.1016/j.ribaf.2024.102361
10. Dwivedi, Y.K., Hughes, L., Kar, A.K., Baabdullah, A.M., Grover, P., Abbas, R., & Wade, M. (2022). Climate change and COP26: Are digital technologies and information management part of the problem or the solution? An editorial reflection and call to action. *International Journal of Information Management, 63.* https://doi.org/10.1016/j.ijinfomgt.2021.102456
11. Ghosh, M. (2024). Financial inclusion studies bibliometric analysis: Projecting a sustainable future. *Sustainable Futures,* 100160. https://doi.org/10.1016/j.sftr.2024.100160
12. Javaid, M., Haleem, A., Singh, R.P., Suman, R., & Khan, S. (2022). A review of Blockchain Technology applications for financial services. *BenchCouncil Transactions on Benchmarks, Standards and Evaluations, 2*(3), 100073. https://doi.org/10.1016/j.tbench.2022.100073
13. Mariano, E. B., Ferraz, D., & de Oliveira Gobbo, S. C. (2021). The Human Development Index with Multiple Data Envelopment Analysis Approaches: A Comparative Evaluation Using Social Network Analysis. *Social Indicators Research, 157,* 443-500. https://doi.org/10.1007/s11205-021-02660-4
14. Nambisan, S. (2017). Digital entrepreneurship: Toward a digital technology perspective of entrepreneurship. *Entrepreneurship Theory and Practice, 41*(6), 1029–1055. https://doi.org/10.1111/etap.12254
15. Nishant, R., Kennedy, M., & Corbett, J. (2020). Artificial intelligence for sustainability: Challenges, opportunities, and a research agenda. *International Journal of Information Management, 53*. https://doi.org/10.1016/j.ijinfomgt.2020.102104
16. Osiyevskyy, O., Umantsiv, Y., & Biliavska, Y. (2023). Digital Ecosystem: A Mechanism of Economic Organization of Enterprises of the Future. *Rutgers Business Review, 8*(2), 175-194. https://rbr.business.rutgers.edu/author/oleksiy-osiyevskyy
17. Onopriienko, K., Lovciová, K., Mateášová, M., Kuznyetsova, A., & Vasylieva, T. (2023). Economic policy to support lifelong learning system development & SDG4 achievement: Bibliometric analysis. *Knowledge and Performance Management, 7*(1), 15-28. http://dx.doi.org/10.21511/kpm.07(1).2023.02
18. Papagiannidis, S., & Marikyan, D. (2022). Environmental sustainability: A technology acceptance perspective. *International Journal of Information Management, 63,* 102445. https://doi.org/10.1016/j.ijinfomgt.2021.102445

19. Pazaitis, A., Kostakis, V., & Bauwens, M. (2017). Digital economy and the rise of open cooperativism: the case of the Enspiral network. *Transfer, 23*(2), 177–192. https://doi.org/10.1177/1024258916683865

20. Pinto, S.O., & Sobreiro, V.A. (2022). Literature review: Anomaly detection approaches on digital business financial systems. *Digital Business, 2*(2), 100038. https://doi.org/10.1016/j.digbus.2022.100038

21. Prokopenko, O., Garafonova, O., & Zhosan, H. (2023). Digital tools in human resource management: how digitization affects personnel management. *Socio-Economic Relations in the Digital Society, 4*(50), 84-94. https://doi.org/10.55643/ser.4.50.2023.540

22. Remeikiene, R., Gaspareniene, L., Fedajev, A., & Vebraite, V. (2021). The role of ICT development in boosting economic growth in transition economies. *Journal of International Studies, 14*(4), 9-22. https://doi.org/10.14254/2071-8330.2022/14-4/1

23. Yankovoi, R., & Sembiyeva, L. (2023). Financial instruments in the development of business innovations. *Socio-Economic Relations in the Digital Society, 4*(50), 5-15. https://doi.org/10.55643/ser.4.50.2023.534

24. Saif, M.A., Hussin, N., Husin, M. M., Muneer, A., & Alwadain, A. (2024). Beyond conventions: Unravelling perceived value's role in shaping digital-only banks' adoption. *Technological Forecasting and Social Change, 203,* 123337. https://doi.org/10.1016/j.techfore.2024.123337

25. Saud, M., Ida, R., Mashud, M., Yousaf, F.N., & Ashfaq, A. (2023). Cultural dynamics of digital space: Democracy, civic engagement and youth participation in virtual spheres. *International Journal of Intercultural Relations, 97*, 101904. https://doi.org/10.1016/j.ijintrel.2023.101904

26. Shestack, Y., Biliavska, Y., Osetskyi, V., Mykytenko, N., & Umantsiv, Y. (2023). Devising a comprehensive method to manage digital competencies. *Eastern-European Journal of Enterprise Technologies, 3,* 86–97. https://doi.org/10.15587/1729-4061.2023.281933

27. Varga, S., Brynielsson, J., & Franke, U. (2021). Cyber-threat perception and risk management in the Swedish financial sector. *Computers & security, 105,* 102239. https://doi.org/10.1016/j.cose.2021.102239

28. von Briel, F., Davidsson, P., & Recker, J. (2018). Digital technologies as external enablers of new venture creation in the IT hardware sector. *Entrepreneurship Theory and Practice, 42*(1), 47–69. https://doi.org/10.1177/1042258717732779

29. Yerina, A., Honchar, I., & Zaiets, S. (2021). Statistical Indicators of Cybersecurity Development in the Context of Digital Transformation of Economy and Society. *Science and Innovation, 17*(3), 3–13. https://doi.org/10.15407/scine17.03.003

30. Zaban, R., & Plaut, P. (2024). The relationship between activities performed in the physical and digital spheres: Lessons learned from the COVID-19 pandemic. *Sustainable Cities and Society,* 106, 105370. https://doi.org/10.1016/j.scs.2024.105370

Білявський В., Білявська Ю., Уманців Ю., Шестак Я., Журба О., Хаванов А.

ЦИФРОВІ ТЕХНОЛОГІЇ У ФІНАНСОВОМУ СЕКТОРІ ЕКОНОМІКИ

Стаття присвячена дослідженню основних тенденцій розвитку цифрових технологій у фінансовому секторі економіки, а саме актуальній темі в умовах: стрімкої глобалізації, диджиталізації та переходу до цифрових екосистем. Сучасний фінансовий сектор економіки на різних стадіях життєвого циклу не може функціонувати без використання цифрових технологій. Крім того, онлайн-активність, перегляд соціальних мереж, web-сторінок і користування різноманітними додатками – це те, без чого не існує громадянське суспільство. Мета роботи полягає в дослідженні зміни впливу перспективних технологій на цифрову безпеку, а також обґрунтування тенденцій розвитку цифрових технологій у фінансовому секторі економіки. Гіпотеза дослідження зосереджена на формуванні потреби в розширенні компетенцій щодо цифрової грамотності, оскільки еволюціонування національної свідомості супроводжується трансформаційними процесами в різних царинах соціальних взаємовідносин, а фінансові аспекти є невід'ємною частиною життєдіяльності й громадян, і бізнес-середовища. У статті застосовано такі науково-емпіричні методи, як причиново-наслідковий аналіз і синтез, дедукція та індукція, систематизація та узагальнення, а також системний і процесний підходи.

У статті охарактеризовано ризики, які виникають унаслідок цифровізації економіки: результати проведеного аналізу свідчать про те, що ефективне використання цих факторів може стимулювати підвищення конкурентоспроможності фінансових установ. Досліджено рівень загрози при управлінні даними, які слід ураховувати при здійсненні прогнозування потенційних загроз цифровізації у фінансовому секторі економіки, що дозволяє керівництву установ оптимізувати фінансові, людські й технологічні ресурси для управління ризиками та вжити заходів щодо нівелювання можливих збитків від кіберзагроз і відновлення стабільного розвитку економічних систем.

Визначено тенденції розвитку цифрових технологій у фінансовому секторі економіки, які потребують детального опрацювання та передбачають здійснення переходу на сучасну цифрову фінансову платформу. Цей перехід не тільки дасть змогу посилити внутрішній ринок країни, підвищуючи рівень незалежності від імпорту зарубіжних тех-

DOI: 10.55643/fcaptp.4.57.2024.4444

нологій, а й сприятиме покращенню світової значущості економіки. Тому застосування цифрових технологій у фінансовому секторі економіки має ключове значення, а ефективне фінансування в умовах нової економічної реальності значною мірою забезпечує успішність соціально-економічного розвитку держави. Стрімкий перехід до повної цифрової трансформації дозволяє відчути й позитивні, й негативні наслідки для фінансового сектора економіки. Громадянське суспільство не готове відмовитися від зручностей, які забезпечують «високі» технології, але недооцінює виникнення потенційних загроз, що пов'язані з інформаційною безпекою. Тому дотримання тенденцій розвитку цифрових технологій та основних цифрових трендів у фінансовому секторі економіки, а також формування дієвих екосистем дозволяють прискорити й оптимізувати управлінські процеси.

Ключові слова: цифровий детокс, безпека даних, цифровізація, візія, управління, фінанси, економіка країни

JEL Класифікація: M20, M21, M59, C80