https://www.sworldjournal.com/index.php/swj/article/view/swj34-03-107
DOI: 10.30888/2663-5712.2025-34-03-107

**УДК 658:338.246**

# DEVELOPMENT OF THE USE OF DIGITAL TECHNOLOGIES IN THE FORMATION OF A MODEL OF SAFETY-ORIENTED MANAGEMENT OF THE ORGANIZATION

## РОЗВИТОК ВИКОРИСТАННЯ ЦИФРОВИХ ТЕХНОЛОГІЙ ПРИ ФОРМУВАННІ МОДЕЛІ БЕЗПЕКООРІЄНТОВАНОГО УПРАВЛІННЯ ОРГАНІЗАЦІЄЮ

**Halhash M.R. / Галгаш М.Р.**
*Postgraduate student, PhD candidate*
*Volodymyr Dahl East Ukrainian National University,*
*Kyiv, Ioann Pavlo II str. 17, Kyiv, 01042*
*Східноукраїнський національний університет імені Володимира Даля,*
*Київ, Іоанна Павла II, 17, 001042*

***Abstract.*** *With the development of digital technologies and artificial intelligence in the modern world, which is experiencing digital transformation, research into the development of the use of digital technologies in security management and their direct impact on the formation of a model of safety-oriented management is becoming increasingly relevant. In the context of the globalization of technological progress and the growth of the level of threats, this topic is gaining strategic importance for the state, business and society as a whole. Digital technologies are increasingly becoming a key tool in the field of security. They allow you to automate management processes, predict potential threats, minimize risks and analyze large volumes of data. In addition, the use of artificial intelligence, Blockchain and cloud technologies provides a new level of control and adaptability of security systems.*

*In addition to the advantages, there are also challenges, such as: cyber threats, privacy threats and adaptation of the regulatory framework to the new realities of modernity, which requires taking these factors into account when developing a comprehensive model of safety-oriented management, which will combine traditional risk management methods with innovative digital methods used by modern companies and leading countries of the world.*

*These are the issues that are proposed to be considered. We will analyze modern technologies in the field of security, consider their capabilities and limitations, and also propose approaches to increasing efficiency when developing a model of safety-oriented management taking into account digital technologies. The main components that play a key role in the formation of a model of safety-oriented management are big data (Big data), artificial intelligence (AI) and Blockchain.*

***Key words:*** *organizational management, safety orientation, safety-oriented management, digital technologies, blockchain, big data, AI, artificial intelligence, management, synergy of technologies.*

## Introduction.

In the context of the rethinking of globalization processes, which is taking place against the backdrop of significant geopolitical transformations in the world, digital and information technologies remain almost the only constant and stable factor in the development of society and relations. At the same time, the current set of political decisions from the world's leading countries, such as trade wars, protectionism and

migration restrictions, do not yet mean the end of globalization, but certainly indicate its transformation. This global transformation is taking place in the following key areas: a shift from full liberalization and global trade agreements towards supporting bilateral agreements and protecting the national industry of countries; a return to economic nationalism: trends towards "friendshoring" and "reshoring"; the development of other forms of globalization (international trade, investments, digital flows and cultural exchange have not disappeared, but are becoming more fragmented, with increasing geopolitical rivalry between leading countries). Thus, humanity is currently witnessing a significant rethinking of the globalization process with an increase in the influence of politics and geopolitics, a decrease in the overall level of security, an increase in the priorities of protecting national interests, and an increase in the role of digital technologies as a key factor in development.

Under such conditions, digital technologies play one of the key roles in the transformation of all spheres of activity of countries and individual organizations. The development of information and communication systems, the widespread implementation of cloud technologies, artificial intelligence, data analytics tools and Big data, Blockchain technologies - provide new opportunities for increasing the efficiency of the management system. At the same time, all these trends are accompanied by an increase in the complexity of risks and threaten the security of organizations.

The issue of developing the use of digital technologies in security systems is becoming particularly relevant in the context of increasing cyber threats, regulatory pressure, high dynamics of changes in the external environment, and increasingly growing requirements for transparency. The lack of a systematic approach to integrating digital technologies into security management systems leads to fragmented solutions, ineffective risk management, and reduced trust in the organization as a whole.

Problem statement. In today's world of rapid digitalization and the growth of various threats, the issue of organizational security takes on a new meaning. Traditional approaches to security management no longer provide the proper level of protection

when the enterprise becomes a complex information system, and technologies, data and people are integrated into a single information and communication ecosystem. Organizations are faced with the need to develop new management models based on the principles of proactive security, adaptability and digital resilience. Despite the availability of various digital solutions, such as AI, Blockchain and Big data, their integration into the safety-oriented management system remains fragmented and not always consistent with the overall development strategy of the organization. There is also a shortage of scientifically based approaches to the formation of an effective management model that would effectively combine digital technologies with an organizational security culture, regulatory framework and risk management systems.

Under such conditions, ensuring the development of the use of digital technologies in the formation of a model of safety-oriented management of the organization becomes an important scientific and practical problem, the solution of which depends on the functioning and development of the economy and society as a whole. The formation of approaches to the integration of modern solutions into the safety-oriented management system, taking into account the risks, requirements and goals of the organization, must be carried out on the basis of combining modern digital technologies, such as Blockchain, Big data and AI, into a single system that works in synergy and interacts for the greatest efficiency of the security system.

**Analysis of recent research and publications.**

Many scientists have paid attention to the study of the development of the use of digital technologies in the formation of a model of safety-oriented management of the organization. Among the Ukrainian scientists who have studied this issue, it is worth noting the following: O. Bernazyuk [47], T. Byrkovich [48], T. Shabatura [49], O. Pankratova [50]. Among foreign scientists, the following can be noted: Dominika Marciniak, Karolina Szymaniec-Mlicka and Hanna Kelm [51], who studied the use of digital technologies in crisis management, as well as Zhe Zhang [52], who studied the impact of digital technologies on security systems and management, and Helen Margetts [53], who analyzed digital democracies and their impact on government decision-making.

The purpose of the article is to study the development of the use of digital technologies in the formation of a safety-oriented management system.

Research results. Significant changes occurring in all spheres of human activity, the development of production factors and economic relations as a result of another technological revolution require corresponding changes in the system of management of organizations. These changes are reinforced by a significant increase in instability and danger factors in the modern world. Given the need to develop the use of digital technologies in the formation of a model of safety-oriented management, as well as modeling a system of interaction of these technologies that would take into account all its main components and ensure stability and adaptability in the organization system.

Humanity gained good experience in developing adaptability and implementing rapid changes in the management system of various systems during the COVID-19 pandemic. In Ukraine, the use of digital technologies not only contributed to solving the problem of the spread of the virus, in particular the "Diya" system, which helped to ensure the functioning of important functions for the state during quarantine restrictions. Quarantine restrictions have given a significant impetus to the comprehensive spread of digital technologies, in particular, the requirements for citizens to have a vaccination certificate (with the possibility of its verification) have given a powerful impetus to its use in smartphones. Digital technologies have become widespread in the field of education and science: online and offline distance learning in educational institutions of various levels (schools, colleges, technical schools, higher education institutions, etc.); online remote holding of scientific conferences, dissertation defenses, etc. The practice of their use has already become commonplace [1].

An important prerequisite for studying the development of the use of digital technologies in the formation of a model of safety-oriented management of an organization is the definition of a structural model and areas of analysis.

The issue of defining a structural model of safety-oriented management of an organization has already been considered by us when defining the typology of organization management according to areas of interest and direction of activity and

structuring the issues of forming safety-oriented management in organizations [54].

When analyzing the methods of implementation and further synergy of digital technologies in the safety-oriented management system, we will take as a basis the structural model widespread in scientific and educational literature, in particular in [9], on which we will rely (Fig. 1).

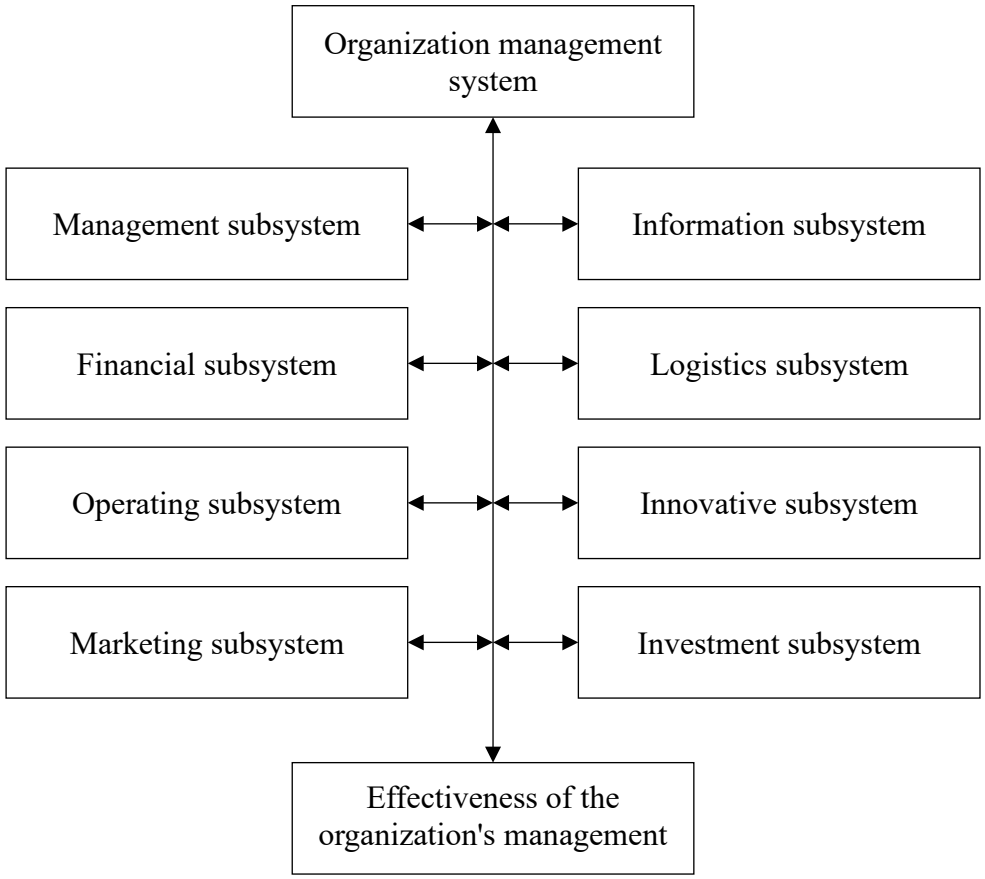


**Figure 1 - The main subsystems of the organization's management**

*Source: [9, p. 22]*

From this diagram, it can be seen that eight main subsystems are considered in the management of the organization. It is necessary to define each of them in order to understand the interpretation of each subsystem:

- the management subsystem provides organization, coordination, planning and control of the organization's activities, implementing key management functions;
- the financial subsystem is responsible for the formation, distribution and use of the organization's financial resources to achieve its strategic and short-term goals;
- the operational subsystem covers the main production and service processes

associated with the creation of goods or the provision of services;

- the marketing subsystem is focused on market research, demand generation, product promotion and maintaining relationships with consumers;
- the information subsystem provides the collection, processing, storage and transmission of information necessary for effective management;
- the logistics subsystem manages material flows, including supply, warehousing, transportation and distribution of products;
- the innovation subsystem is engaged in the development and implementation of new products, technologies, processes that contribute to increasing competitiveness;

The investment subsystem is responsible for planning, attracting and effective use of investment resources for the development of the organization [9].

Regarding the issue of determining the directions of analysis of the development of the use of digital technologies in the formation of a model of safety-oriented management of the organization, we will proceed from the following assumptions. Digital technologies in the formation of a safety-oriented management system can be considered and applied in a variety of ways, however, the intellectual analysis of the information space using AI made it possible to single out from the whole variety of modern approaches, digital tools and technologies those that are most effectively used today in the field of management such technologies as Big data, Blockchain and AI are used, as those that have a certain set of tools and have experience of using in practice by various organizations, and can also work both autonomously and together.

The synergy of the above digital technologies in the organization's management system is designed to form an intelligent, decentralized and adaptive security system capable of effectively responding to threats. This opens up new opportunities for management at different levels, ensuring the functioning of critical infrastructure, ensuring the stability, flexibility and reliability of the security system.

To perform an intellectual analysis on the development of the use of digital technologies in the formation of a model of safety-oriented management of the organization, we have developed a scheme of synergy of Big data, Blockchain and AI (Fig. 2).

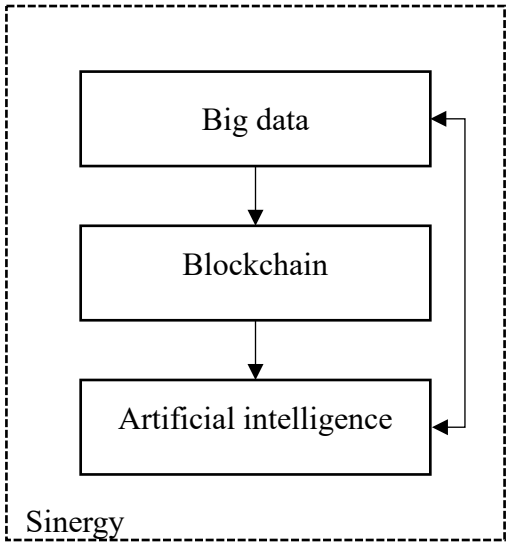


**Figure 2 - Synergy of the development of the use of digital technologies in the system of safety-oriented management of organizations**

*Author's development*

Big data, Blockchain and AI should work in synergy to increase the efficiency of the functioning of the safety-oriented management model, as modern digital technologies without which it is not possible to create any security model.

Therefore, the results of the intellectual analysis and forecasting of the development of the use of digital technologies in the formation of a safety-oriented management model of the organization according to the specified structural model, which includes eight subsystems of organization management (see Fig. 1) and three areas of analysis (Big data, Blockchain and AI).

Regarding the methodology of the study, to analyze data on the development of the use of digital technologies in the formation of a safety-oriented management model of the organization, an analysis was carried out using the tools AI-driven Data Analysis, Machine Learning-based Analytics, Predictive Analytics, Big Data Analytics with AI. The analysis of the development of the use of digital technologies in the formation of a safety-oriented management model of the organization was carried out on real statistical data. As an information space, sites, reports, and open access databases were considered, which provide data on the implementation of digital technologies in the subsystems of organizations, in particular [10-17, 33-34, 42-46].

1. Results of analysis and forecasting of the development of the use of Big data in safety-oriented management of the organization.

One of the key factors in security management is the use of Big data and cloud storage. Big data is an important factor, since the capabilities for collecting, analyzing, and transferring large volumes of data and technologies are increasing with the advent of modern tools for working with data, such as business intelligence. The capabilities of collecting, analyzing data, and reporting using a large set of tools and methods have increased dramatically with the emergence of business intelligence tools, competitive intelligence, dashboards, information panels, data warehouses, data mining, and big data, which have appeared relatively recently and have changed our daily activities in general [2, p. 3]. With these tools, it becomes possible to provide them, in the presence of large data sets, for business, the state or any organization, it gives the opportunity to better protect against theft or damage to data by using cloud storage, but also the danger of cyber threats appears, which can lead to the inoperability of large data sets and data leakage. Accordingly, this creates both opportunities and corresponding threats.

A vivid example is the experience of leading countries in the world, such as the USA or China, whose special services and other state security institutions, with the capabilities of ensuring digitalization, were able to create large data servers on which information is stored and secure data from attacks by criminals and intelligence agencies of other countries. However, over time, new types of threats have appeared, according to which groups of, so to speak, “state cybercriminals or “white hackers” were created in these same services and institutions, working in the interests of the governments of a particular state. Accordingly, the capabilities of Big data provided opportunities at the beginning of its development to secure their data by storing them on servers, but over time, the number of threats of data loss and leakage increased, an example is the Wikileaks website, which posted a lot of secret information from the US and UK governments, which led to social tension and scandals. Thus, Big data provides both great opportunities and great threats of dissemination and leakage of information by cybercriminals, but still, governments do not undertake to return to previous means of data storage, for example, in archives and other physical media -

this is a perfect example that, with all its shortcomings, storing data on servers is still more secure than on physical media, and accordingly more effectively secures data from the encroachments of criminals. Examples of such Ukrainian tools are “Diya” or state registers, which were transferred to electronic servers, although they were repeatedly attacked by cybercriminals, but storage on servers still turned out to be more effective.

Thus, the use of cloud technologies and Big data allows you to secure and make possible the existence of any security system, since the effectiveness of the functioning of this system directly depends on the capabilities of working with data.

In Fig. 1, you can see the main subsystems of most organizations, based on it and using statistical data from reliable and scientifically relevant sources, a forecast was developed that approximates the growth in the use of Big data in percent, see table. 1.

**Table 1 - Forecast of the implementation of Big data into the management system of organizations at the level of each subsystem**

| Year / Subsystem | 2025 | 2026 | 2027 | 2028 | 2029 | 2030 |
|---|---|---|---|---|---|---|
| Operational | 50% | 55% | 60% | 65% | 70% | 75% |
| Marketing | 45% | 50% | 55% | 60% | 65% | 70% |
| Financial | 60% | 65% | 70% | 75% | 80% | 85% |
| Information | 55% | 60% | 65% | 70% | 75% | 80% |
| Management | 35% | 40% | 45% | 50% | 55% | 60% |
| Logistics | 40% | 45% | 50% | 55% | 60% | 65% |
| Innovation | 30% | 35% | 40% | 45% | 50% | 55% |
| Investment | 50% | 55% | 60% | 65% | 70% | 75% |

*Developed with the use of sources: [42-46]*

It is also necessary to separately investigate the benefits that Big data provides in each subsystem of the organization's management for its implementation. By studying scientific works in various fields, Table 2 was prepared.

**Table 2 - Advantages of implementing Big data into the organization's management system, at the level of each subsystem**

| Subsystem | Benefits of implementing Big data into the subsystem |
|---|---|
| Management | Increasing information awareness of management entities: Big data helps to make more informed strategic decisions, optimize business processes, improve risk management and increase control effectiveness. Identifying trends: Data analytics allows you to identify trends, predict future events and identify key strategic threats and success factors.<br>Increasing the level of decision-making efficiency: The use of Big data can improve the decision-making process, as it becomes possible to identify patterns and trends in financial data [35-36]. |
| Financial | Improving risk management: Big Data makes it possible to identify financial risks and develop an action plan to minimize them [35]. |
| Operational | Data analysis and processing: Big data plays an important role in enabling the analysis of large data sets, including real-time data, which are difficult to analyze using traditional methods without human error risks [37]. |
| Marketing | Trend detection: Big data helps to identify new trends, analyze market needs, generate new ideas, and accelerate the process of developing new products and services [38]. |
| Information | Increasing information availability: The rapid development of Big Data capabilities has made information more accessible, but at the same time more difficult to manage. This leads to the need to develop a clear strategy and implement information management policies in the organization [39]. |
| Logistics | Increased transparency: Big data can improve the transparency and quality of service management in the logistics industry. Through the open exchange of logistics information and data sharing, visualized flowcharts and dashboards are created that promote information transparency [40]. |
| Innovation | Innovative technologies for process improvement: Big data plays an important role in the development of technologies such as Blockchain and AI, which can be used in fintech companies to improve decision-making and automate processes.<br>Increased innovation capabilities: An important aspect is information management, which positively affects the connection between big data analytics capabilities and a firm's broad innovation capabilities [36, 39]. |
| Investment | Investment forecasting: With Big Data tools, organizations can track and analyze market data, social media sentiment analysis, and geopolitical events to predict market movements and adjust investment strategies accordingly to prevent risks to the organization. In addition, predictive models can be continuously updated with real-time data, allowing for dynamic and adaptive risk assessment [41]. |

As you can see, modern data analytics and Big data tools provide broad opportunities for automation and large-scale and structural data analytics, which contributes to more efficient operation of the safety-oriented management system as a whole and separately at different levels of the organization's management subsystems.

2. Results of analysis and forecasting of the development of the use of Blockchain in safety-oriented management of the organization.

An important problem when working with data is anonymity. The use of automated technologies, such as machine learning, can lead to the disclosure of the user's identity through simple inference or direct random visibility. This data must be anonymous for client safety [3, p. 57]. Therefore, cybersecurity and Blockchain technology are no less important components. The use of appropriate encryption technologies to protect communication data is a rather important and integral component of digital technologies in the safety-oriented management system, since the level of security of this model depends on it, and Blockchain ensures transparency, immutability and reliability of information. Blockchain technologies have many advantages in providing data encryption for any system, therefore they are used in most leading companies and government organizations. The main advantages of this technology are decentralization, immutability and transparency, security, which is possible through crypto encryption, which makes forgery impossible [7, 8].

Blockchain technologies are already used in such important institutions as electoral institutions and many management systems. For example, electronic voting systems are already being created in many countries to increase the transparency of elections. Also, in healthcare, to preserve medical confidentiality and exchange data between institutions. In addition, in logistics and supply, to track goods in real time. In finance, the use of Blockchain technologies has gained importance, since such cryptocurrencies as Bitcoin and Ethereum work on their basis. Thus, due to its advantages, Blockchain continues to develop and increasingly cover new areas of public life. Therefore, the formation of a safety-oriented management system without taking into account Blockchain technology is complicated, since it is a very important component of security for any system.

In Fig. 1, you can see the main subsystems of most organizations, based on it and using statistical data from reliable and scientifically relevant sources, a forecast was developed that approximates the growth in the use of Blockchain technologies in percent, see table. 3. When developing this forecast, risks and deviations were taken into account, by taking into account negative scenarios. Two scientific sources with an expert assessment of development trends were analyzed.

**Table 3. Forecast of the implementation of Blockchain technologies into the management system of organizations at the level of each subsystem [33-34]**

| Year / Subsystem | 2025 | 2026 | 2027 | 2028 | 2029 | 2030 |
|---|---|---|---|---|---|---|
| Operational | 25% | 30% | 35% | 40% | 45% | 50% |
| Marketing | 15% | 20% | 25% | 30% | 35% | 40% |
| Financial | 40% | 50% | 60% | 70% | 80% | 90% |
| Information | 30% | 35% | 40% | 45% | 50% | 55% |
| Management | 20% | 25% | 30% | 35% | 40% | 45% |
| Logistics | 35% | 45% | 55% | 65% | 75% | 85% |
| Innovation | 25% | 30% | 35% | 40% | 45% | 50% |
| Investment | 30% | 40% | 50% | 60% | 70% | 80% |

*Developed with the use of sources: [33-34]*

From table. 3 you can see the trend of implementing Blockchain technologies at the level of various subsystems of the organization's management. The financial, logistics and investment subsystems have the highest rates of implementation of Blockchain, due to the already developed Blockchain tools in these areas.

It is also necessary to separately investigate what advantages Blockchain technology provides in each subsystem of the organization's management for its implementation. Studying scientific works in various fields, table. 4 was made.

Thus, Blockchain technologies contribute to the protection of the management subsystem and play one of the key roles in the modern safety-oriented management system, as they guarantee data protection, reliable security and encryption.

**Table 4 - Advantages of implementing Blockchain technologies into the organization's management system, at the level of each subsystem**

| Subsystem | **Advantages of implementing Blockchain technologies into the subsystem** |
|---|---|
| Management | Decentralization of management: Blockchain provides the opportunity to create DAOs (Decentralized Autonomous Organizations), which operate on the basis of smart contracts, automating the process of management and decision-making. This helps to reduce bureaucracy and increase transparency. |

| | |
|---|---|
| | Secure data storage: Important management documents and records can be stored using Blockchain, ensuring their immutability and protection against forgery.<br>Improving the level of corporate governance: Blockchain promotes transparency and accountability in management, simplifying auditing and control [8]. |
| Financial | Simplifying payments and transactions: Blockchain allows for fast and secure transactions without intermediaries, reducing fees and speeding up processes.<br>Asset tokenization: Real assets (real estate, stocks, etc.) can be represented as tokens on the Blockchain, simplifying their circulation and management.<br>Decentralized finance (DeFi): Blockchain is the basis for DeFi platforms, which offer alternative financial services, such as lending, deposits, and insurance, without the involvement of traditional financial institutions [28]. |
| Operational | Supply chain management: Blockchain provides transparency and traceability of goods at all stages of the supply chain, from production to consumer.<br>Process automation:<br>Smart contracts can automate contract execution and other operational processes.<br>Efficiency improvement: Blockchain reduces the need for manual data processing and paper documentation, increasing operational efficiency [29]. |
| Marketing | Transparency and Trust: Blockchain allows for transparent and verifiable records of products and services, which increases consumer trust. For example, companies can use Blockchain to track the origin of food products, demonstrating their safety and quality.<br>Direct connection with brands: Blockchain allows companies to interact directly with consumers, bypassing intermediaries such as advertising agencies. This allows for more personalized and relevant marketing campaigns [28]. |
| Information | Data Security: Blockchain provides a high level of data security due to its decentralized and encrypted nature. This makes it difficult for unauthorized access, modification, or deletion of information. Mughayar emphasizes that Blockchain can be particularly useful for storing sensitive data, such as medical records or financial information.<br>Transparency and Immutability: Records in Blockchain are immutable, meaning they cannot be changed or deleted without a trace. This increases transparency and accountability in an organization. Mughayar gives the example of using Blockchain to track supply chains, where every stage of a product's movement is recorded in Blockchain, allowing consumers to verify its origin and authenticity.<br>Data Exchange Efficiency: Blockchain simplifies the exchange of data between different parties, eliminating the need for intermediaries. This can significantly speed up business processes and reduce costs. Mughayar considers the example of using Blockchain to simplify international payments, where transactions can be made directly between banks without the involvement of correspondent banks [30]. |
| Logistics | Improved transparency and traceability: Blockchain enables the tracking of goods at every stage of the supply chain, from the manufacturer to the end consumer. This increases transparency and allows for the rapid identification and resolution of issues related to the movement of goods. Example: Tracking pharmaceuticals to prevent counterfeiting and ensure their authenticity.<br>Simplify processes and reduce paperwork: Blockchain enables the automation of many logistics processes, such as document processing and customs clearance. This reduces the need for paper documentation and speeds up information processing. Example: Automating the process of issuing bills of lading, which significantly reduces the time and cost of delivering goods.<br>Optimize inventory management: Blockchain can help optimize inventory management by allowing companies to accurately track the number of goods in warehouses and forecast demand. Example: Automatically ordering goods when their quantity in the warehouse reaches a certain level [31]. |

| | |
|---|---|
| Innovation | New business models based on Blockchain: Blockchain can facilitate the emergence of new business models based on decentralization, transparency and automation. This can open up new opportunities for innovation and the creation of new products and services. Changing the role of intermediaries: Blockchain can reduce the need for intermediaries in various industries, which can lead to new, more efficient ways for companies to interact with customers. This can stimulate innovation by creating new opportunities for direct interaction with customers [32]. |
| Investment | Democratization of Investment: Blockchain lowers the barriers to entry into the investment market, allowing small investors to participate in projects that were previously only available to large investors.<br>Cost reduction and efficiency improvement: Blockchain automates many investment processes, such as calculations and document verification. This reduces transaction costs and increases the efficiency of investment activities [30]. |

3. Results of analysis and forecasting of the development of the use of AI in safety-oriented management of the organization.

The next component is AI and machine learning. AI is becoming increasingly relevant in any industry, and cannot but affect the field of safety-oriented management as well. Machine learning is an important component of artificial intelligence, which allows any artificial neural network to develop and gain experience gradually. Firstly, AI can act as an arbitrator who solves problems in the safety-oriented management system and makes it possible to make a particular decision as an unbiased and independent expert who does not have a subjective opinion on the relevant event, individual, proposal and makes the most appropriate decision for any subjects of the dispute. Accordingly, any AI can be automated to analyze relevant behavioral models and detect anomalies in security systems.

AI can also help optimize management decisions based on relevant predictive analytics, since modern technologies using artificial intelligence allow for automatic fast analytics. In addition, it can work in management arbitration as a separate entity that can be given the authority to make certain decisions. In examples of the use of artificial intelligence in developed and leading organizations, it is already given certain powers by management, such as: forming SMART goal models, conducting SWOT analysis, resolving conflicts, etc.; in this example, it can also be used in a safety-oriented management system for greater efficiency and minimizing the risks of the human factor in decision-making.

The use of artificial intelligence in security management systems has quite broad

potential. Firstly, the potential for creating various training programs and trainings, which are created for personnel and management with the help of artificial intelligence. Moreover, with the help of artificial intelligence, this gives the prospect of maximally updating information with each subsequent release of new products and innovations in the field of activity. Secondly, AI opens up opportunities for creating various simulations that can be created with its help and get a unique experience of simulating threats and risks for the organization, as well as testing scenarios without real risk for the organization. Thirdly, AI can act as an arbitrator for resolving conflicts in the organization, since conflicts in the organization can also be considered as a threat to a particular organization, its existence. In addition, AI may be able to analyze the emotional climate in the organization by analyzing internal information and finding certain problems, with its development and inevitable implementation in modern cybernetics and other technologies. Thus, AI can be configured appropriately and involved specifically for the purpose of analyzing and resolving internal conflicts, and even reacting accordingly to the emergence of conflicts. Similarly, artificial intelligence is capable of offering a variety of scenarios for resolving these conflicts and offering them to members of the organization, as scenarios from the side of an independent arbitrator, as well as being a virtual mediator, which will be agreed to be relied upon as an entity that can have the powers of an independent arbitrator and mediator, since AI is able to assess the decisions and actions of members of the organization as objectively as possible, and to what extent this or that action of an individual member of the organization may pose a threat, be unlawful, may cause conflict and have negative consequences for the organization, etc. Accordingly, AI is also able to develop certain policies, recommendations and rules of conduct for overcoming such conflict situations, which will be adapted to the environment of a specific organization.

In Fig. 1 shows the main subsystems of most organizations, based on it and using statistical data from reliable and scientifically relevant sources, a forecast was developed that approximates the growth in the use of artificial intelligence in percentage terms, see Table 5.

**Table 5 - Forecast of the introduction of artificial intelligence into the management system of organizations at the level of each subsystem**

| Year / Subsystem | 2025 | 2026 | 202 | 2028 | 2029 | 2030 |
|---|---|---|---|---|---|---|
| Operational | 45% | 55% | 65% | 75% | 80% | 85% |
| Marketing | 40% | 50% | 60% | 70% | 75% | 80% |
| Financial | 35% | 45% | 55% | 65% | 70% | 75% |
| Information | 30% | 40% | 50% | 60% | 65% | 70% |
| Management | 25% | 35% | 45% | 55% | 60% | 65% |
| Logistics | 20% | 30% | 40% | 50% | 55% | 60% |
| Innovation | 15% | 25% | 35% | 45% | 50% | 55% |
| Investment | 10% | 20% | 30% | 40% | 45% | 50% |

*Developed with the use of sources: [10-17]*

The forecast was made on the basis of information from open sources, taking into account the implementation of similar technologies, trends, by applying linear and exponential extrapolation, taking into account expert opinion and taking as a basis the average positive development scenario, however, it should still be considered conditional and the main conclusion from this forecast is the overall growth of implementation in all specified subsystems of the organization's management.

The table shows the share of organizations in percentages that have implemented AI in subsystems. From this summary table, which is made on the basis of several scientific studies, one can see significant growth dynamics in all subsystems of organizations. As can be seen, AI will be most effectively used in the operational and marketing subsystem, this is due to the already developed tools in these subsystems and extensive experience in using artificial intelligence in these areas, as well as the ease of its implementation in these subsystems. The smallest percentage is precisely the innovation and investment subsystems, this is due to high risks and unpredictability of results, and complexity due to a wide range of various processes in these subsystems, however, it should be noted their very rapid growth dynamics, which is associated with the further development of artificial intelligence, which will lead to rapid growth dynamics.

It is also necessary to separately investigate what benefits AI provides in each subsystem of the organization's management for its implementation. Studying scientific works in various fields, Table 6 was made.

**Table 6 - Advantages of implementing artificial intelligence into an organization's management system, at the level of each subsystem**

| Subsystem | **Advantages of implementing artificial intelligence into a subsystem** |
|---|---|
| Management | Decision support: AI helps analyze large amounts of data and provide recommendations for strategic decision-making, resource optimization, and risk management. Automation of routine tasks: AI can automate administrative tasks, which simplifies the work of managers so that they can focus more on strategic issues[18]. |
| Financial | Financial risk management: AI can be used to conduct stress testing and creditworthiness assessments.<br>Fraud and financial risk detection: Machine learning algorithms can analyze transactions and other data to identify potential risks and alert an organization's financial managers to them. This can help reduce financial losses and protect the organization's reputation [19, 20, 21]. |
| Operational | Automation of routine tasks: AI automates routine tasks, leading to increased efficiency and reduced operational costs.<br>Service personalization: AI is used to personalize services to increase customer satisfaction and loyalty [22]. |
| Marketing | Detailed analysis: AI allows for the analysis of large amounts of customer data (demographics, online behavior, purchase history) to create detailed profiles, preventing errors and threats that organizations face due to the human factor.<br>Increased relevance: AI allows marketers of organizations to personalize content, offers and recommendations, increasing relevance for each customer.<br>Improved marketing tools: AI improves advertising targeting, ensuring that ads are shown only to those users who are most likely to be interested in a product or service [23]. |
| Information | Data analytics: AI can analyze large amounts of data and identify important trends and patterns.<br>Cybersecurity: AI can detect and prevent cyberattacks by analyzing network traffic and detecting anomalies [24]. |
| Logistics | Route optimization: AI helps determine optimal delivery routes, taking into account factors and threats such as traffic, weather conditions, weight and volume restrictions. Threat and risk prediction: AI can also predict possible delays and suggest alternative routes [25]. |
| Innovation | Developing new products and services: AI can analyze customer demand data and market trends to develop new products and services.<br>Automation of research and development: AI can automate some stages of research and development, accelerating the innovation process [26]. |
| Investment | Asset Price Forecasting: AI can be used to build predictive models that analyze historical data and other factors to predict future prices of stocks, bonds, currencies, and other assets to reduce both long-term and short-term financial risks for an organization. Portfolio Optimization: AI can be used to optimize an investment portfolio, taking into account various factors such as risk, return, and diversification [27]. |

It can be concluded that AI reduces risks and threats for each subsystem of the organization's management and positively contributes to the work of the safety-oriented management system as a whole.

However, there are also certain threats when forming and implementing artificial intelligence into the safety-oriented management model. An example is the solution of the trolley dilemma by artificial intelligence [5, 6]. Thus, an AI must be trained that will comply with basic human principles, ethical norms and principles of humanity, which will solve problems and make decisions in accordance with the interests of a certain community, the safety of which is the key goal of the existence of the safety-oriented management system. However, this creates problems with its full implementation into such a model, until such an AI is trained that will have the corresponding high ethical and moral principles, which are rationality.

Given the existing potential and challenges facing the state, the most priority areas for the development of artificial intelligence in Ukraine should be considered production and defense [4], in which a safety-oriented management system can be directly implemented.

Thus, the development of the use of Big data, Blockchain and AI in safety-oriented management of the organization will allow to increase the level of security and ensure effective risk monitoring and automate the process of risk and threat management. AI is able to analyze large amounts of information in real time, predict risks and automate management decision-making in management arbitration. It is able to automatically detect threats and automate behavioral patterns and detect anomalies that indicate potential threats, as well as recognize faces and identify biometrically, contributing to the security of access to critical security systems. In addition, it is capable of intelligent forecasting, analyzing information from previous experience and developing risk forecasting models in the field of cybersecurity, personnel management, industrial safety, etc. It is capable of advanced event analysis, analyzing large data sets from sensors, video surveillance cameras, information systems, for rapid response to threats.

Blockchain technologies provide transparency of data protection and reduce the

risks of unauthorized access to information security systems. Blockchain can be used to record all events, create a secure event registry in the security system, which ensures their immutability and availability for appropriate audit and verification. Also, thanks to Blockchain, the use of smart contracts is available for automatic execution of security measures, such as blocking access when threats are detected. Blockchain technologies allow you to protect data from hacking and internal threats, through decentralized storage of confidential data, and also guarantees the integrity of information and makes it impossible to forge data, which is critically important when forming a safety-oriented management system [7, 8].

Big data allows you to effectively process information about threats and model scenarios of relevant risks. Analysis of large data sets to identify patterns helps to recognize potential threats and weaknesses in security systems. Big data also helps to process large amounts of data in real time. Monitoring systems using Big data can quickly detect and analyze threats based on streaming data. Integrating information from various sources, such as video surveillance, sensors, analytical reports, to obtain a complete picture of risks, thanks to which Big data methods make it possible to correlate different data sources. This makes it possible to use analytics to improve the efficiency of security management systems, based on preliminary analysis of incidents through optimization of management decisions.

The combination of these technologies makes it possible to create their synergy: artificial intelligence, Blockchain technologies and Big data in safety-oriented management, and to form not just a safety-oriented management system, but an innovative system that will be adaptive, transparent and secure. It will work as follows: AI analyzes and predicts risks, Big data structures and integrates information, and Blockchain technology ensures data security and its reliability. Such a model will allow you to quickly respond to threats, minimize the human factor and increase the effectiveness of security measures in state, corporate management, the public sector and any other management system, which makes it universal. The implementation of these technologies will help make the security system intelligent, automated and reliable, which is a key task of the modern safety-oriented management system. In

addition, the synergy of the joint use of Big data, Blockchain and AI technologies in safety-oriented management of the organization makes it possible to provide both substantive and functional information protection, in particular, certain data sets are encrypted and protected by Blockchain technology from changes, and only then, using artificial intelligence, processing, analytics and other data operations are automated and optimized. Functioning together, AI, modern analytics and data processing technologies, thanks to Blockchain as a means of their protection and encryption, create synergy.

**Conclusions.** In today's dynamically transforming digital environment, the use of digital technologies is becoming not just a trend, but a strategic necessity to ensure effective and adaptive safety-oriented management of an organization. The conducted research proves that it is the synergistic combination of artificial intelligence, Big data and Blockchain technology that forms a sustainable innovative management model that is able to respond to current challenges, security and risks in real time. AI provides automation of processes, risk analysis, threat detection and decision-making; is based on machine learning and its built-in forecasting algorithms. Big data allows you to process large amounts of information, obtaining the necessary information for a prompt response. Blockchain, in turn, guarantees transparency, immutability and security of information, which is important in the context of security and the level of trust in the organization.

The developed model of synergy of these technologies is not only a tool for increasing the effectiveness of the organization's security system, but also the basis and foundation for building a new management paradigm that combines innovations with traditional approaches to minimizing risks. This approach allows organizations not only to respond to threats, but also to proactively form security strategies, taking into account global, technological and regulatory changes. Thus, the role of digital technologies in the formation of a safety-oriented management system is decisive, and their integration into a single functional system opens up new opportunities for sustainable, reliable and effective security management in the context of digital transformation.

**References**

1. Ilyashenko S. M., Shipulina Yu. S., Ilyashenko N. S. Management of innovative development in the context of technological transformations: monograph. Sumy: Tritoria, 2023. 228 p.

2. Introduction / M. Cöster et al. Digital Transformation. Cambridge, UK, 2023. P. 1–24. URL: https://doi.org/10.11647/obp.0350.01 (accessed: 29.03.2025).

3. Use of big data in hacking and social engineering. Big Data Security. 2019. P. 47–74. URL: https://doi.org/10.1515/9783110606058-004 (accessed: 29.03.2025).

4. Strategy for the development of artificial intelligence in Ukraine: monograph / A. I. Shevchenko et al. [Edited by A. I. Shevchenko]. Kyiv: IPSHI, 2023. 305 p.

5. Sommaggio, Paolo, and Samuela Marchiori. "Moral dilemmas in the AI era: A new approach." Journal of Ethics and Legal Technologies 2.JELT-Volume 2 Issue 1 (2020): 89-102.

6. Liao S. M. A Short Introduction to the Ethics of Artificial Intelligence. Ethics of Artificial Intelligence. 2020. P. 1–42. URL: https://doi.org/10.1093/oso/9780190905033.003.0001 (accessed: 29.03.2025).

7. Ramya H. P., Hemalatha K. G. Blockchain Revolution. Handbook of Digital Innovation, Transformation, and Sustainable Development in a Post-Pandemic Era. Boca Raton, 2024. P. 105–119. URL: https://doi.org/10.1201/9781003438748-6 (accessed: 29.03.2025).

8. Swan M. Blockchain: Blueprint for a New Economy. O'Reilly Media, Incorporated, 2015.

9. Nazarchuk T. V., Kosiyuk O. M. Organizational Management: Textbook. Kyiv: Center for Educational Literature, 2016. 560 p.

10. Deloitte. Tech Execs Expect Growth in 2024 [Electronic resource]. – Access mode: https://deloitte.wsj.com/cio/tech-execs-expect-growth-in-2024-133d523d

11. Bain & Company. Generative AI is now virtually ubiquitous in global businesses [Electronic resource]. – Access mode: https://www.bain.com/about/media-center/press-releases/2024/generative-ai-virtually-ubiquitous-in-global-business-as-the-technology-spreads-at-a-near-unprecedented-rate--bain--company-proprietary-

survey

12. Boston Consulting Group (BCG). AI Adoption in 2024: 74% of Companies Struggle to Achieve and Scale Value [Electronic resource]. – Access mode: https://www.bcg.com/press/24october2024-ai-adoption-in-2024-74-of-companies-struggle-to-achieve-and-scale-value

13. KPMG. Transforming the enterprise of the future [Electronic resource]. – Access mode: https://kpmg.com/xx/en/media/press-releases/2024/06/tansforming-the-enterprise-of-the-future.html

14. PwC. 2025 AI Business Predictions [Electronic resource]. – Access mode: https://www.pwc.com/ua/en/survey/2024/ai-predictions.html

15. McKinsey & Company. Gen AI adoption: The next inflection point [Electronic resource]. – Access mode: https://www.mckinsey.org/capabilities/people-and-organizational-performance/our-insights/gen-ais-next-inflection-point-from-employee-experimentation-to-organizational-transformation

16. Statista. Responsible AI adoption in organizations 2024 [Electronic resource]. – Access mode: https://www.statista.com/statistics/1465383/responsible-ai-adoption-in-organizations

17. European Court of Auditors. Artificial intelligence: EU must pick up the pace [Electronic resource]. – Access mode: https://www.eca.europa.eu/ECAHTMLNews/NEWS-SR-2024-08/en/body.html

18. Davenport T. H. Only Humans Need Apply: Winners and Losers in the Age of Smart Machines [Electronic resource] / T. H. Davenport. – Leaders Excellence, 2016. – August 18. – Access mode: https://leadersexcellence.com/wp-content/uploads/dlm_uploads/2016/08/Davenport-Leaders-Excellence-presentation.pdf.

19. Zetzsche D. A., Buckley R. P., Arner D. W., Tang, B. Artificial Intelligence in Finance: Putting the Human in the Loop [Electronic resource] / D. A. Zetzsche, R. P. Buckley, D. W. Arner, B. Tang - 2019. - Access mode: https://ac-landing-pages-user-uploads-production.s3.amazonaws.com/0000049303/50dc584c-9034-445f-a459-84aecbd28829.pdf

20. Sheng C., Qian H., Mo M. China Credit-Tech Market Report: Technology-Driven Value Generation in Credit-Tech [Electronic resource] / C. Sheng, H. Qian, M. Mo. - Oliver Wyman & China Securities Credit Investment Company, 2019. - Access mode: https://www.oliverwyman.com/content/dam/oliver-wyman/v2/publications/2019/apr/china-credittech-market-report-4.pdf.

21 Agrawal A., Gans J., Goldfarb A. Prediction Machines: The Simple Economics of Artificial Intelligence. - Boston: Harvard Business Review Press, 2018. - 272 p.

22. Cherian A. T. Transforming Operations Management with Artificial Intelligence [Electronic resource] / A. T. Cherian. - University of Essex, 2024. - Access mode: https://www.researchgate.net/publication/377974349_Transforming_Operations_Management_with_Artificial_Intelligence.

23. Davenport T., Guha A., Grewal D., Bressgott T. How artificial intelligence will change the future of marketing [Electronic resource] / T. Davenport, A. Guha, D. Grewal, T. Bressgott // Journal of the Academy of Marketing Science. – 2019. – Access mode: https://doi.org/10.1007/s11747-019-00696-0.

24. Iansiti M., Lakhani K. R. Competing in the Age of AI: Strategy and Leadership When Algorithms and Networks Run the World [Electronic resource] / M. Iansiti, K. R. Lakhani. - Boston: Harvard Business Review Press, 2020. - Access mode: https://www.hbs.edu/faculty/Pages/item.aspx?num=56633.

25. Pillac V., Gendreau M., Guéret C., Medaglia A.L. A review of dynamic vehicle routing problems // European Journal of Operational Research. - 2013. - Vol. 225, Issue 1. – P. 1–11. - DOI: 10.1016/j.ejor.2012.08.015.

26. Cockburn I.M., Henderson R., Stern S., The Impact of Artificial Intelligence on Innovation: An Exploratory Analysis // ResearchGate. – 2023. – URL: https://www.researchgate.net/publication/365176813_The_Impact_of_Artificial_Intelligence_on_Innovation_An_Exploratory_Analysis.

27. Jansen S. Machine Learning for Algorithmic Trading: Predictive Models to Extract Signals from Market and Alternative Data for Systematic Trading Strategies with Python. – 2nd ed. - Birmingham: Packt Publishing, 2020. - 800 p. - ISBN 978-1-

83921-771-5.

28. Tapscott D., Tapscott A. Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World. - New York: Penguin Random House, 2016. - 368 p. - ISBN 978-1-101-90363-2.

29. Saberi S., Kouhizadeh M., Sarkis J., Shen L. Blockchain technology and its relationships to sustainable supply chain management // International Journal of Production Research. - 2019. - Vol. 57, No. 7. – P. 2117–2135. - DOI: 10.1080/00207543.2018.1533261.

30. Mougayar W. The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology. - 1st ed. - Hoboken, NJ: Wiley, 2016. - 208 p. - ISBN 978-1-119-30031-1.

31. Wamba S.F., Ben-Daya M., Youssef H. Blockchain Technology in Logistics: A Conceptual Model and Empirical Findings // International Journal of Production Economics. - 2019. - Vol. 211. – P. 239–252. – DOI: 10.1016/j.ijpe.2019.01.011.

32. Treiblmaier H. The Impact of Blockchain Technology on Business Models: A Literature Review and Future Research Agenda // Supply Chain Management: An International Journal. - 2018. - Vol. 23, Issue 6. – P. 619–639.

33. Grand View Research. Blockchain Technology Market Size, Share & Trends Analysis Report By Type (Public Cloud, Private Cloud), By Offering (Platform, Services), By Component, By Application, By Enterprise Size, By End-use, By Region, And Segment Forecasts, 2025-2030. - San Francisco: Grand View Research, 2025. - 130 p. – URL: https://www.grandviewresearch.com/industry-analysis/blockchain-technology-market.

34. Fortune Business Insights. Blockchain Technology Market Size, Share & Industry Analysis, By Component (Platform/Solution and Blockchain as a Service), By Type (Public, Private, Hybrid, and Consortium), By Application (Digital Identity, Payments, Smart Contracts, Supply Chain Management, Internet of Things (IoT), and Others), By Deployment (Proof of Concept, Pilot, and Production), By Industry (BFSI, Energy & Utilities, Government, Healthcare and Life Sciences, Manufacturing, Telecom, Media & Entertainment, Retail & Consumer Goods, Travel and

Transportation, and Others), and Regional Forecast, 2025–2032. - San Francisco: Fortune Business Insights, 2025. - 160 p.

35. Davenport T.H., Barth P., Bean R. How 'Big Data' Is Different // MIT Sloan Management Review. - 2012. - Vol. 54, No. 1 (Fall). – P. 22–24. – (Big Idea: Competing With Data & Analytics). – URL: https://sloanreview.mit.edu/article/how-big-data-is-different/.

36. Mhlanga D. The Role of Big Data in Financial Technology Toward Financial Inclusion // Frontiers in Big Data. - 2024. - Vol. 7. – Article 1184444. – DOI: 10.3389/fdata.2024.1184444. – URL: https://www.frontiersin.org/articles/10.3389/fdata.2024.1184444/full.

37. Mittal S., Khan M.A., Romero D., Wuest T. Smart Manufacturing: Characteristics, Technologies and Enabling Factors // Proceedings of the Institution of Mechanical Engineers, Part B: Journal of Engineering Manufacture. - 2019. - Vol. 233, No. 5. – P. 1342–1361. - DOI: 10.1177/0954405417736547.

38. Manyika J., Chui M., Brown B., Bughin J., Dobbs R., Roxburgh C., Byers A.H. Big Data: The Next Frontier for Innovation, Competition, and Productivity. - Washington: McKinsey Global Institute, 2011. - 156 p. – URL: https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/big-data-the-next-frontier-for-innovation

39. Mikalef P., Boura M., Lekakos G., Krogstie J. The Role of Information Governance in Big Data Analytics Driven Innovation // Information & Management. - 2020. - Vol. 57, Issue 8. – Article 103361. – DOI: 10.1016/j.im.2020.103361.

40. Wang Y., Feng L., Chang H., Wu M. Research on the Impact of Big Data on Logistics // Journal of Management and Engineering. - 2017. - Vol. 1, No. 1. – P. 12–19. – URL: https://www.researchgate.net/publication/314783431_Research_on_the_Impact_of_Big_Data_on_Logistics.

41. Olaiya O. P., Cynthia A. C., Usoro S. O., Obani O. Q., Nwafor K. C., Ajayi O. O. The impact of big data analytics on financial risk management // International Journal of Science and Research Archive. - 2024. - Vol. 12, No. 2. – P. 821–827. -

DOI: 10.30574/ijsra.2024.12.2.1313.

42. Sharma R. Big Data Technology Market Report: Global Forecast from 2025 to 2033 / R. Sharma. - Dataintelo, 2024. - 293 p. – URL: https://dataintelo.com/report/global-big-data-technology-market

43. Fortune Business Insights. Big Data Technology Market Size, Share & Industry Analysis, By Type (Big Data Storage, Big Data Mining, Big Data Analytics, and Big Data Visualization), By End-use Industry (BFSI, Retail, Manufacturing, IT and Telecom, Government, Healthcare, and Others), and Regional Forecast, 2024–2032 [Electronic resource]. — Fortune Business Insights, 2025. — Access mode: https://www.fortunebusinessinsights.com/industry-reports/big-data-technology-market-100144

44. Market Research Future. Investment Opportunities of Big Data Technology Market Research Report: By Application (Healthcare, Retail, Financial Services, Manufacturing, Telecommunications), By Deployment Type (On-Premises, Cloud-Based, Hybrid), By Technology (Artificial Intelligence, Machine Learning, Data Analytics, Data Mining), By End Use (Small Enterprises, Medium Enterprises, Large Enterprises) and By Regional (North America, Europe, South America, Asia Pacific, Middle East and Africa) – Forecast to 2035 [Electronic resource] / Aarti Dhapte. — Market Research Future, May 2025. — 128 p. — Access mode: https://www.marketresearchfuture.com/reports/investment-opportunities-of-big-data-technology-market-42883

45. AGEST Vietnam. Big Data Trends for 2025: Emerging Innovations [Electronic resource] / AGEST Vietnam. — 2024. — Access mode: https://www.agest.vn/blogs/big-data-trends-for-2025/

46. Grand View Research. Big Data Market Size To Reach $862.31 Billion By 2030 [Electronic resource]. — Grand View Research, Inc., January 2025. — Access mode: https://www.grandviewresearch.com/press-release/global-big-data-market

47. Bernaziuk O. Administrative E-Services: Concept and Conditions of Implementation in Ukraine / O. Bernaziuk // Entrepreneurship, Economy and Law. – 2019. – No. 5. – P. 196–199. – DOI: https://doi.org/10.32849/2663-5313/2019.5.36.

48. Byrkovych T. I., Byrkovych V. I., Kabanets O. S. Mechanisms of Public Governance in the Field of Digital Transformations // Public Administration: Improvement and Development. – 2019. – No. 9. – URL: https://journals.maup.com.ua/index.php/public-management/article/view/2463/2934

49. Strelkovskyi V., Gryshova I., Kalyuhina S. Modern Technologies in Public Administration: A Comparison of Estonia, India, and the United Kingdom [Electronic Resource] // Revista „Administratie si Management Public". — 2017. — No. 28. — P. 174–185. — Access Mode: https://www.ceeol.com/search/article-detail?id=720037

50. Pankratova O. M. Digitalization as a Modern Trend in Management Development [Electronic Resource] / O. M. Pankratova // Economy and Society. — 2021. — No. 33. — P. 336–341. — Access Mode: https://economyandsociety.in.ua/index.php/journal/article/view/927

51. Marciniak D., Szymaniec-Mlicka K., Kelm H. New Technologies in Crisis Management // Journal of Public Governance. – 2023. – Vol. 65, No. 3. – P. 73–85. – DOI: https://doi.org/10.15678/PG.2023.65.3.06

52. Zhang Z., Guo H.W.B., Chang-Richards A., Jin R., Han Y. Digitalisation-Based Situation Awareness for Construction Safety Management – A Critical Review // Proceedings of the 38th International Symposium on Automation and Robotics in Construction (ISARC 2021). – 2021. – Vol. 38. – P. 605–612

53. Dunleavy P., Margetts H., Bastow S., Tinkler J. Digital Era Governance: IT Corporations, the State, and E-Government // OUP Catalogue. – 2006. – Oxford University Press

54. Halhash M. R. Issues of forming safety-Oriented management in organizations // Bulletin of the Volodymyr Dahl East Ukrainian National University. – 2024. – No. 4 (284). – P. 5–14

***Анотація.*** *З розвитком цифрових технологій та штучного інтелекту в сучасному світі, який переживає цифрову трансформацію все більше стають актуальними дослідження розвитку використання цифрових технологій у менеджменті безпеки та безпосередньо їх вплив при формуванні моделі безпекоорієнтованого управління. За умов глобалізації технологічного прогресу та зростання рівня загроз ця тема набуває стратегічного значення для держави, бізнесу та суспільства в цілому. Цифрові технології стають все більше ключовим інструментом у сфері безпеки. Вони дозволяють автоматизувати управлінські*

*процеси, передбачувати потенційні загрози, мінімізувати ризики та здійснювати аналіз великих обсягів даних. Крім того, використання штучного інтелекту, Blockchain та хмарних технологій забезпечує новий рівень контролю і адаптивності систем безпеки.*

*Окрім переваг, виникають і виклики, такі як: кіберзагрози, загрози конфіденційності й адаптації нормативної бази до нових реалій сучасності, що вимагає у сукупності враховувати ці фактори при розробки комплексної моделі безпекоорієнтованого управління, яка буде поєднувати традиційні методи управління ризиками з інноваційними цифровими методами які використовуються сучасними компаніями та провідними державами світу.*

*Саме ці питання пропонується розглянути. Ми проаналізуємо сучасні технології у сфері безпеки, розглянемо їхні можливості й обмеження, а також запропонуємо підходи щодо підвищення ефективності при розробки моделі безпекоорієнтованого управління з урахуванням цифрових технологій. Основними складовими, які відіграють ключову роль при формуванні моделі безпекоорієнтованого управління є великі дані (Big data), штучний інтелект (далі AI) і Blockchain.*

***Ключові слова:*** *менеджмент організації, безпекоорієнтованість, безпекоорієнтоване управління, цифрові технології, Blockchain, Big data, AI, штучний інтелект, управління, синергія технологій.*

*Науковий керівник: д.е.н., проф. Овчаренко Є.І.*

Статтю надіслано: 25.11.2025 р.