The object of this study is the process of assessing the level of information potential of energy enterprises under the conditions of digital coherence. The problem of effective management of the information potential of energy enterprises is solved on the basis of devising a methodology for assessing the level of information potential of energy enterprises under the conditions of digital coherence, taking into account modern challenges associated with the integration of digital systems. The methodology makes it possible to ensure the accuracy of analysis, prompt decision-making, and adaptation to the dynamic conditions of digital transformation. The devised methodology is based on interrelated stages, including the integration of indicators, assessment of the interaction of system components, and monitoring changes in indicators of the information potential of energy enterprises. The main stages of the methodology are selection of components of the information potential, such as the level of automation, IT infrastructure, staffing, information security, and digital systems; analysis of their interaction; monitoring and management of risks in real time. It was determined that the application of the methodology makes it possible to identify the weaknesses of the enterprise's information system and adapt it to new challenges, including cyber threats and the need for technological updates. The main feature is the ability of the methodology to analyze the relationships between infrastructure components, taking into account digital coherence, which makes it possible to increase the accuracy of risk assessment and the efficiency of managing the information potential of the energy enterprise. Based on the data obtained, it is possible to assess the critical decrease in the level of information potential of the Zaporizhzhia Power Plant from 0.5790 to 0.3710 arbitrary units and its possible consequences for the efficiency of the enterprise

Keywords: information potential, energy enterprises, integral indicator, digital coherence, assessment of information potential

UDC 658.5:004.9
DOI: 10.15587/1729-4061.2025.332324

DEVISING A METHODOLOGY FOR ESTIMATING THE INFORMATION POTENTIAL OF ENERGY ENTERPRISES UNDER THE CONDITIONS OF DIGITAL COHERENCY

Viktoriia Prokhorova
Doctor of Economic Sciences, Professor*
Oleksandr Budanov
PhD Student*
Pavlo Budanov
Corresponding author
PhD, Associate Professor
Department of Electrical Engineering and Power Engineering**
E-mail: pavelfeofanovich@ukr.net
Krystyna Slastianykova
Assistant*
*Department of Economics and Management**
**V. N. Karazin Kharkiv National University
Svobody sq., 4, Kharkiv, Ukraine, 61022

Received 03.04.2025
Received in revised form 01.05.2025
Accepted 09.06.2025
Published 30.06.2025

How to Cite: *Prokhorova, V., Budanov, O., Budanov, P., Slastianykova, K. (2025). Devising a methodology for estimating the information potential of energy enterprises under the conditions of digital coherency. Eastern-European Journal of Enterprise Technologies, 3 (13 (135)), 6–16. https://doi.org/10.15587/1729-4061.2025.332324*

1. Introduction

In the context of digital transformation, energy enterprises are faced with new challenges that necessitate effective management of information potential. This potential serves as the basis for ensuring competitiveness, innovative development, adaptation to market changes and technological modernization. It is advisable to consider it as an independent economic category that includes not only information resources but also software, digital infrastructure, methods of data collection, processing, and analysis.

Despite current theoretical and methodological advancements, under present-day conditions there is no unified methodology for assessing information potential that would fully take into account the specificity of digital transformation in the energy industry. Existing approaches are fragmented, overly subjective, often focused only on individual technical or organizational aspects, which reflects the complete picture of the enterprise's information development.

The main problems are the difficulty of selecting relevant indicators, the lack of a single integrated indicator, and insufficient consideration of such digital aspects as the level of information potential of enterprises and interaction with the external information environment. This complicates the process of making strategic decisions, managing risks, and implementing new technologies.

The proposed methodology should include an analysis of such components as the structure and interconnections of the information infrastructure; the level of use of modern technologies; the degree of automation and digital security; the ability to scale and adapt systems.

Particular attention is paid to the analysis of interconnections between elements of the digital infrastructure, which makes it possible to assess potential risks, identify vulnerabilities, model the consequences of implementing new technologies, and increase the efficiency of information flow management. The methodology should also take into account the current level of digital integration of the enterprise with the ability to form predictive models for strategic planning.

The integration of cybersecurity tools, analysis of large volumes of data, use of cloud platforms and artificial intelligence systems will significantly expand the possibilities of information potential management. This creates the prerequisites for a prompt response to threats, minimizing risks, and improving the efficiency of the energy enterprise.

2. Literature review and problem statement

The identification of four main areas of enterprise digitalization (cloud technologies, data management, data analytics, artificial intelligence) demonstrates the depth of analysis in work [1]. However, the complexity of analytical tools can reduce their clarity, especially for government suppliers and small enterprises. It is also not enough to consider the practical aspects of implementing new technologies in less developed markets, which may leave out conventional methods that are still relevant for some enterprises.

In [2], an approach to improving enterprise information management is considered, using blockchain as a tool that allows integration with cloud and edge computing. This makes it possible to optimize and scale blockchain applications, ensuring their competitiveness. However, the complexity of implementing blockchain technology can be difficult to understand and integrate, especially for less technologically advanced enterprises. In addition, the use of different approaches and solutions can cause incompatibility between blockchain systems.

In [3], various supporting information technologies, such as digital twins, collaborative robots, and the Internet of Things, are analyzed, which facilitate the adaptation of new concepts. The importance of the human factor in interaction with high-tech solutions is noted, which enhances the innovative potential. However, the complexity of integration in the use of new technologies, such as edge computing, can be difficult to implement, especially for small and medium-sized businesses. In addition, the increasing reliance on human-machine collaboration can create new risks associated with technology failures or insufficient training of personnel.

In paper [4], the implementation of digital tools for managing the information potential of enterprises is considered. However, the technology faces numerous difficulties in integrating into already established industries and practices.

In [5], the application of modern information methods and digital tools to ensure information security is analyzed, through semantic analysis and identification of ways to avoid dangerous threats. However, current methods are often theoretical in nature and practically untested, which reduces their effectiveness in the real information environment. In addition, a comprehensive analysis of user information paths and behavior models may require significant resources and technical competence. At the same time, research results are not always adapted to real-world applications.

In paper [6], the role of critical infrastructure is considered. It is shown that smart grids based on digital technologies are key to the modernization of energy systems, increasing their efficiency, reliability, and integration. At the same time, significant attention is paid to research and development of solutions to protect smart grids from cyberattacks, which helps reduce risks to the information potential of enterprises. However, smart grids have a complex structure, which can complicate their implementation and management. In addition, despite research and countermeasures, systems remain vulnerable to violations of confidentiality, integrity, or availability of data.

Work [7] reports a study on factors forming an information security culture, which is the basis for the sustainable development of the information potential of enterprises. The advantage is the practical focus of the research and the structured nature of the conclusions; the disadvantage is a limited sample of respondents.

Study [8] proposes a structural analysis of the information security standardization process, which is of great importance for the formation of a stable information potential of enterprises. The strengths are the originality of the theoretical approach, and the weakness is the complexity of adapting the model to practice.

In [9], the impact of moral alienation and counterproductive behavior on employees' awareness of information security, which directly affects the sustainability of information potential, was investigated. The advantage is that it takes into account the psychological aspects of risk, but the results have limited generalizability.

Paper [10] emphasizes the key role of cyber-physical systems and big data in implementing autonomous solutions for innovation in manufacturing. It is shown that continuous data collection by cyber-physical systems provides the basis for improving the scalability and information potential of enterprises. Currently, implementing solutions that combine these technologies can require significant resources and specialized knowledge. However, the large amount of data generated can create risks for confidentiality and information security. In addition, studying the interaction of cyber-physical systems and big data limits potential practical applications.

Work [11] highlights the role of artificial intelligence in solving complex problems, such as the climate crisis, by reducing the use of natural resources and the energy intensity of human activity. However, machine learning models are often based on historical data, which can limit their flexibility and accuracy, and also require enhanced protection of data and information systems.

In works [12, 13], it is proposed to consider the information potential of an enterprise at three levels, which characterize the existing level of information development and an integral assessment of the total information potential of the enterprise. The feasibility of determining the level of information development of an industrial enterprise in two aspects is proven: as the potential for interaction with the external information environment and as production information potential. However, the choice of three levels may not fully cover all aspects of information potential, especially if the specific operating conditions of energy enterprises are not taken into account. In addition, the assessment may not take into account rapid changes in the information environment or technologies that affect the development of the information potential of the enterprise.

The characteristics of existing methodologies for assessing information potential in works [1–13] showed the following advantages and disadvantages.

The advantages of methodologies for assessing information potential include:

– completeness, since information potential is considered from the point of view of ensuring information activity of all structural divisions of the enterprise;

– structuredness, since a set of indicators is given that determine the development of information potential of enterprises;

– modifiability, since it is possible to vary sets of indicators in blocks depending on the type of enterprise activity;

– complexity, which offers a system of indicators for assessing the information potential of interaction with internal information flows and external information space;

– visibility, since it allows for a graphic display of the integral value of information potential, which determines the level of its development.

The disadvantages of methodologies for assessing information potential are:

– most of the indicators of the proposed system characterize the organizational side of information potential, without taking into account the productive component;

– the possibility of subjective assessment is not excluded since expert assessments of individual indicators are used;

– the methodology is based on an absolute approach to assessing information potential, which makes the value of the potential dependent on the size of the enterprise;

– incomplete methodological elaboration since no interpretation of the resulting assessment of information potential is provided;

– narrow focus of the methodologies;

– expert assessment of the significance of parameters does not exclude the subjectivity of the resulting integral indicator.

These shortcomings indicate the need to devise integrated approaches to assessing the level of information potential of energy enterprises, taking into account digital coherence.

Despite significant achievements in the area of research into the information potential of energy enterprises, there are a number of unresolved problems related to its assessment in the context of digital coherence:

– the lack of a single methodology that does not make it possible to take into account the complex impact of digital technologies on all levels of information potential management;

– there is a lack of a generalized model that would cover all aspects of digital coherence, such as data integration, system interaction, and forecasting;

– the analysis of information potential components is often carried out in isolation, without taking into account their synchronization and mutual influence in digital systems;

– digital coherence requires an assessment of end-to-end relationships, which still remains a fragmented task.

– the constant development of digital technologies creates new opportunities but also complicates the modeling and forecasting of information potential;

– the problem of adapting methodologies to rapidly changing conditions has not been solved;

– many existing models focus only on analyzing the current state of information potential, ignoring long-term forecasting of risks and opportunities, which makes it difficult to identify risk areas that may affect management effectiveness;

– although information potential is closely related to security issues, there is often a lack of a systematic approach to their integration with cybersecurity elements;

– the lack of a single platform for managing information potential and security reduces the efficiency of resource use.

Thus, the unsolved nature of these problems indicates the need to devise more advanced and adaptive approaches that would take into account digital coherence, the dynamics of technology development, and the complex interaction between components. This opens up prospects for further scientific research and improvement of existing models.

3. The aim and objectives of the study

The purpose of our study is to devise a methodology for assessing the level of information potential of energy enterprises in the context of digital coherence, which takes into account modern challenges of digital integration and ensures increased efficiency in managing the information potential of energy enterprises. This will make it possible for energy enterprises, taking into account digital coherence, to more effectively integrate new digital technologies and adapt their information systems to new challenges and quickly respond to potential threats and risks.

To achieve the goal, the following tasks were set:

– to define stages in the methodology for assessing the level of information potential of an energy enterprise;

– to verify the methodology on real data of energy enterprises to assess its effectiveness.

4. The study materials and methods

The object of our study is the process of assessing the level of information potential of energy enterprises under the conditions of digital coherence. The assessment of information potential includes the definition of key indicators, analysis of digital infrastructure, level of digital maturity, innovative potential, integration of digital processes, and monitoring of results.

The study focuses on the development of methods for assessing the level of information potential of energy enterprises, taking into account digital coherence. The emphasis is on the definition of key indicators, analysis of digital infrastructure, level of digital maturity and innovative potential, as well as on the integration of digital processes into the activities of the energy enterprise.

The hypothesis of the study assumes that devising a method for assessing the level of information potential of energy enterprises under the conditions of digital coherence could significantly improve the efficiency of information potential management due to the following:

– it would contribute to a more accurate assessment of information potential by taking into account digital and innovative components;

– it could ensure effective integration of digital processes into the activities of energy enterprises;

– it would minimize subjectivity in the assessment process through the use of standardized approaches;

– it could contribute to making strategic decisions based on objective data;

– it would increase the adaptability of enterprises to changes in digital infrastructure and market conditions.

Therefore, the hypothesis suggests that the devised methodology will improve the ability of energy industry enterprises to effectively manage information potential risks and reduce vulnerabilities associated with the integration of digital technologies [14–17]. This will make it possible for enterprises to more effectively use their information potential to increase productivity and competitiveness.

To assess the level of information potential of enterprises, an expert method is used, which allows involvement of specialists to assess the current level of information potential and provide recommendations for its improvement. In addition, this method is used for sophisticated analyses that require professional knowledge and experience.

The use of the expert method is one of the key tools for assessing the information potential of enterprises. Its feature is the use of the professional experience of specialists who are able to deeply analyze the state of the information system and its components.

The main features of the application of the expert method:

– experts analyze not only technical aspects but also organizational and strategic components of information potential;

– the involvement of experts allows for the assessment of complex relationships between components of information potential;

– it covers the analysis of data, technologies, infrastructure, and human resources.

– experts provide not only an assessment but also recommendations for improving the efficiency of using information resources;

– at energy enterprises, the expert method is used to assess the effectiveness of digital platforms, for example, cloud solutions and IoT technologies.

– it identifies critical points: experts assess system components that may pose a risk to the sustainability of the enterprise in the context of digital integration.

– adaptation to change: the method makes it possible to adapt the information potential to new technologies and the challenges of digital transformation.

Owing to the expert method, one can achieve more accurate assessments and form the basis for improving the information potential of energy enterprises.

5. Results of devising a methodology for assessing the level of information potential of energy enterprises under the conditions of digital coherence

5. 1. Development of stages in the methodology for assessing the level of information potential of energy enterprises

Devising a methodology for assessing the level of information potential of energy enterprises under the conditions of digital coherence includes several stages (Fig. 1), each of which has its specific characteristics:

Stage No. 1 – selection of components of information potential. This is an important first step that forms the basis for the development and effective use of information potential. The selection of components determines how the enterprise's information system will be built and what should be emphasized. Usually this begins with an analysis of the needs, resources, and goals of the energy enterprise.

At this stage, it is proposed to select the following components:

– automation level simplifies and accelerates information processes, reduces the amount of manual labor, and increases the economic efficiency of energy enterprises;

– IT infrastructure level includes everything that ensures the operation of information systems (servers, network equipment, software);

– personnel level: these are IT, security, and data analysis specialists who support and develop the information potential of energy enterprises;

– information security level protects information potential from cyberattacks, leaks, and unauthorized access;

– digital systems level: tools and platforms for managing, analyzing, and storing the information potential of energy enterprises.

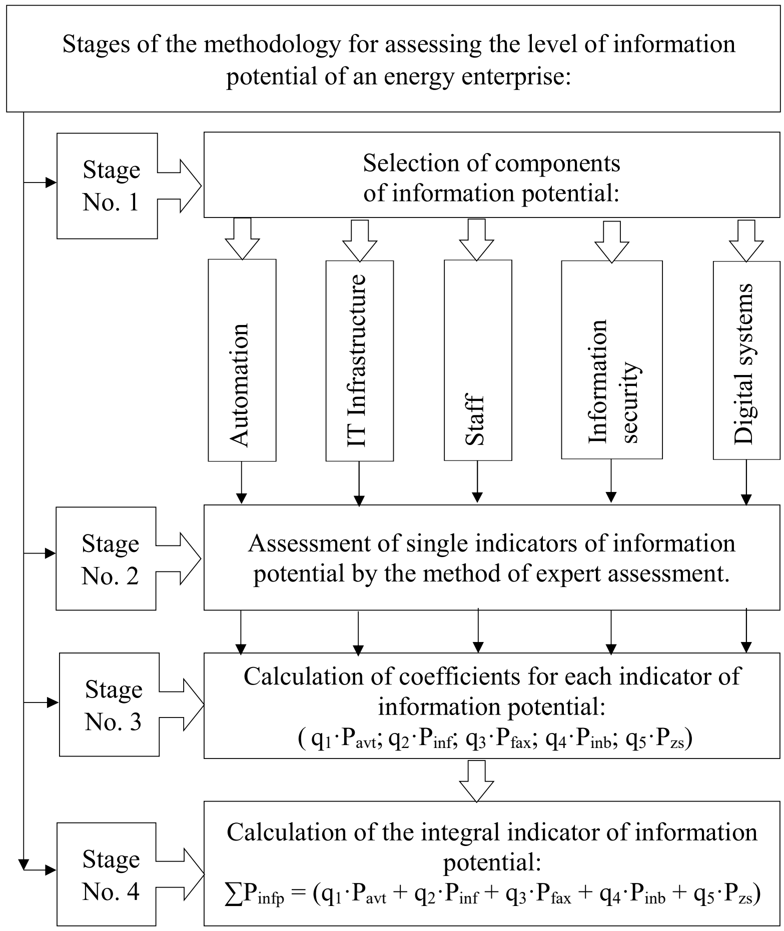

Fig. 1. Stages of the methodology for assessing the level of information potential of an energy enterprise

Stage 2 – assessment of individual indicators of information potential by expert assessment method is a process that makes it possible to quantitatively assess individual aspects of information potential using expert opinions. The main idea is to involve specialists who have deep knowledge in the relevant field to determine the weight or significance of each indicator of information potential of energy enterprises. Experts evaluate each indicator on a specific scale of points (for example, from 0 to 1; from 1 to 10) for further generalization of assessments to obtain an average value or other statistical indicator. This stage makes it possible to take into account the subjective opinions of experts and turn them into objective data that can be used for analysis or decision-making.

Stage 3 – selection and calculation of information potential indicators:

1. Automation level indicator (Pavt): percentage of automated processes at the enterprise. This is one of the most important indicators for determining the level of digitalization, which includes the implementation of automated systems

and processes that make it possible to reduce or eliminate human participation (operational personnel) in performing standard, repetitive tasks. These can be software and hardware solutions that improve the efficiency of the enterprise.

The automation indicator exerts the following impact on the information potential:

– a high level of automation improves the speed and accuracy of operations, reduces labor costs, and reduces errors;

– a low level of automation means that the enterprise does not fully use the potential of technologies to reduce operating costs and improve efficiency.

It is proposed to use the following types of automation indicators: the number of automated workplaces or processes at the energy enterprise; the cost of investments in automation per unit of production or services.

The automation indicator (P_{avt}) of energy enterprises determines the share of automated processes at the enterprise out of the total number of processes. This is an important indicator of the level of digitalization of the energy enterprise, as it demonstrates how effectively the energy enterprise uses modern technologies to optimize and automate its operations. The automation indicator (P_{avt}) of the energy enterprise can be calculated using the following formula (1)

$$P_{avt} = \frac{N_{avtp}}{\sum N_{proz}} \cdot 100\%, \quad (1)$$

where P_{avt} is the automation index of energy enterprises, %;

N_{avtp} – number of automated processes (workplaces) at the energy enterprise;

$\sum N_{pr}$ – total number of processes (workplaces) at the energy enterprise.

A high level of automation index of energy enterprises P_{avt} includes:

– reduction of time and resource costs (automation makes it possible to reduce the time spent on routine tasks, increasing the overall efficiency of the enterprise);

– increased accuracy and reduction of errors (for example, owing to automated systems, the probability of human errors is reduced, which is especially important in areas such as finance, production, logistics, etc.);

– speed of reaction (for example, automated processes work faster, which makes it possible to the enterprise to quickly respond to market changes);

– innovation and scalability (for example, energy companies with a high level of automation are able to implement new technologies faster and scale their operations with minimal personnel costs.

This indicator directly affects the level of information potential of the enterprise. The more processes are automated, the less the enterprise depends on manual labor and the more it is focused on using digital technologies for its activities. A high level of automation indicator indicates that the energy company is able to quickly adapt to technological changes and is ready for future innovations. In general, a high percentage of automated processes is a competitive advantage and an important factor for the success of the enterprise in the digital economy.

2. IT infrastructure indicator (P_{inf}): assessment of the availability of modern IT infrastructure (0 – absent, 1 – modern). This indicator reflects the extent to which the energy enterprise has the necessary equipment to support IT processes.

The IT infrastructure indicator (P_{inf}) includes all technological resources of the energy enterprise: servers, network components, databases, software, data transmission networks and other equipment necessary for the implementation of information processes. The IT infrastructure indicator has the following impact on information potential:

– a developed IT infrastructure provides stable and fast data processing, high reliability of operation, and the ability to scale production;

– an insufficiently developed IT infrastructure can limit the enterprise's capabilities in data processing speed, reduce the level of security and stability of systems.

It is proposed to use the following types of IT infrastructure indicators: network throughput; level of reliability and availability of systems; volume of stored data and capabilities for their processing. It is important that the evaluation criteria are clearly defined and that all participants in the evaluation understand under what conditions a value of 0 or 1 is assigned. It is proposed to define several levels of IT infrastructure indicators:

– P_{inf} =0 – no infrastructure;

– P_{inf} =0.5 – part of the necessary infrastructure is available at the energy enterprise, but not at the modern level;

– P_{inf} =0.75 – part of the necessary infrastructure is available at the modern level;

– P_{inf} =1.0 – full modern infrastructure is available at the energy enterprise.

These levels make it possible to understand in more detail at what stage the enterprise is and what part of the infrastructure needs to be improved.

To determine the IT infrastructure indicator (P_{inf}), the enterprise needs to conduct a detailed assessment of its IT resources according to certain criteria and based on this, assign an appropriate score (0 or 1). Such an assessment will help understand the enterprise's readiness to use modern IT solutions and technologies.

3. IT specialists per 100 people indicator (P_{fax}): it measures the number of IT specialists per 100 employees of the enterprise, which indicates the level of specialization and qualification of employees in the IT field. The more qualified IT specialists there are in the enterprise, the greater its information potential. The IT specialists per 100 people indicator has the following impact on information potential:

– a high number of IT specialists indicates great attention to the development and support of information technologies, which allows for faster adaptation of new technologies;

– a low number of IT specialists may indicate a shortage of technical resources for the development and support of information systems.

It is proposed to use the following types of indicators of IT specialists per 100 people: number of IT specialists per 100 employees; qualifications of IT specialists (for example, availability of certifications, level of education and experience).

Calculation of the number of IT specialists per 100 employees of the enterprise is an important indicator for assessing the information potential of the enterprise. It shows how much the enterprise depends on IT resources and the availability of qualified specialists to ensure the effective operation of information systems (2)

$$P_{fax} = \frac{N_{ITfax}}{\sum N_p} \cdot 100\%, \quad (2)$$

where P_{fax} is the indicator of IT specialists per 100 people;

N_{ITfax} is the number of IT specialists;

$\sum N_p$ is the total number of employees at an enterprise.

The higher the indicator P_{fax}, the more IT specialists are involved in the work of the enterprise, which means a greater potential for the development of information technologies, automation of production processes, and support for innovation. If a large number of IT specialists work at the enterprise, this makes it possible for the enterprise to respond faster to changes in the technological environment, develop its own digital solutions, and effectively implement new technologies.

4. Information security level indicator (P_{inb}) is a set of measures and technologies aimed at protecting information and information systems from unauthorized access, destruction, changes, or theft. This indicator assesses the level of protection of the enterprise's information resources from external and internal threats, such as cyberattacks, data leaks, unauthorized access, malicious programs, etc. The score on a scale from 0 to 10 makes it possible to determine how effectively the enterprise's data and IT systems are protected, and what level of protection it provides. The higher the level, the more reliably the enterprise is protected from cyberattacks. The Information Security Level Indicator (P_{inb}) includes both physical protection (e.g., access control) and software solutions (antivirus software, data encryption, network monitoring). The Information Security Indicator has the following impact on the information potential of enterprises:

– a high level of information security reduces the risks of data loss and disruption of production processes;

– a low level of information security creates threats to the confidentiality, integrity, and availability of data, which can lead to serious financial and reputational losses.

It is proposed to use the following types of information security indicators: the number of security incidents (for example, data leaks); recovery time after an incident; the level of security of information systems (use of standards, certifications).

The assessment of information security on a scale of 0–10 should take into account all these aspects. Each component can be assessed from 0 to 10 points depending on how reliably it is implemented and operates at the energy enterprise. These assessments can then be summed or combined to determine the overall level of protection.

The following methodology for assessing information security levels on a scale of 0–10 points is proposed:

– $P_{inb} = 0–3$ points – low level of information security: minimum level of security measures; no antivirus programs, data protection tools are used; employees do not undergo cybersecurity training, there are no monitoring systems;

– $P_{inb} = 4–6$ points – average level of info security: basic antivirus programs are not always updated; partial data encryption; employees have limited understanding of cyber threats and do not undergo regular training.

– $P_{inb} = 7–8$ points – high level of info security: modern antivirus solutions are used; multi-factor authentication is implemented; employees regularly undergo cybersecurity training; there are automated monitoring systems for possible threats;

– $P_{inb} = 9–10$ points – excellent level of info security:

1) the infrastructure is protected at all levels (physical security, network security, encryption, antivirus);

2) constant monitoring of all IT systems and security incidents;

3) all employees undergo regular cybersecurity training; the latest security technologies are being integrated;

4) fully automated backup and disaster recovery processes;

5) constant updating of security policies and application of best international practices.

The assessment of the information security indicator (0–10) makes it possible to get a clear idea of the level of protection of the enterprise's IT systems. The higher the level, the better the enterprise is protected from cyberattacks, data leaks, and other threats. Using this scale, one can determine where security needs to be improved and what measures should be implemented to reduce risks.

5. Digital systems indicator (P_{zs}): the number of implemented digital systems (on a scale from 0 to 3). This indicator determines how actively the enterprise uses advanced technologies to manage and automate its processes.

The digital systems indicator (P_{zs}) includes software and platforms used to automate management, production, or other industrial processes. These can be both standard systems and specialized solutions for specific production tasks. The digital systems indicator has the following impact on the information potential of enterprises:

– developed digital systems make it possible to significantly increase the economic efficiency of enterprises, provide better communication, convenient access to data and process automation;

– the presence of limited or outdated digital systems can limit the speed of data processing, increase the likelihood of errors and slow down decision-making.

It is proposed to use the following types of indicators of digital information potential systems: the number of digital platforms and programs used in the enterprise; the degree of integration of digital systems with other financial and production systems.

A system of criteria is proposed for assessing the number of implemented digital systems (0–3):

– P_{zs}=0 points: digital systems are not implemented or are not used. Process management is carried out manually without digital systems or using basic tools;

– P_{zs}=1 point: one digital system is implemented, but its use is limited to individual processes (for example, the APCS system of the power unit of the power plant for monitoring technological parameters). Digitalization is at the initial stage;

– P_{zs}=2 points: two digital systems are implemented that are integrated into several key processes (for example, the APCS system of the power unit for managing energy production and the ASKUE system for managing energy distribution). Automation increases efficiency and productivity;

– P_{zs}=3 points: three or more digital systems are widely implemented and integrated into a single enterprise infrastructure, and cover most or all key processes (monitoring, forecasting, maintenance, resource management). High level of automation and efficiency.

Thus, indicators of information potential such as "automation" and "digital systems" help improve the economic efficiency of energy enterprises, reduce costs and time for completing tasks. Indicators of information potential such as "IT infrastructure" and "Info security" ensure stable and secure operation of all digital solutions. Indicators of information potential such as "IT specialists per 100 people" are an important indicator of the availability of sufficient resources to support and develop IT systems, which determines the ability of the enterprise to introduce innovations and adapt to new technologies. These indicators make it possible to assess the level of information potential of an energy enterprise and its ability to effectively use information technologies to achieve economic goals.

These criteria may vary depending on the specificity of energy enterprises and make it possible to objectively assess the level of information potential in the context of enterprise digitalization.

Stage No. 4 – calculation of the integral indicator of the information potential of enterprises by normalizing the indicators (converting them to a relative scale of 0–1); determination of weights (by expert assessment method); calculation of the integral index:

1. Normalization of indicators (conversion into a relative scale from 0 to 1 points). This is necessary so that all indicators of information potential are comparable. Normalization of the indicator (P_N) can be performed by one of the following methods (3)

$$P_N = \frac{P_i - P_{\min}}{P_{\max} - P_{\min}}, \quad (3)$$

where P_N is the normalized indicator of information potential;

P_i - value of the indicator for a specific energy enterprise;

$P_{\min}$ - minimum values of this indicator among all energy enterprises;

$P_{\max}$ - maximum values of this indicator among all energy enterprises;

2. Determination of weight coefficients (q_i) by the method of expert assessment. To this end, a group of experts is invited to assess the importance of each indicator (for example, on a scale from 0 to 1). Then the averaging of estimates and normalization of weights, respectively, are carried out (4)

$$\sum q_i = 1, \quad (4)$$

where q_i is the weight coefficient of the information potential indicator.

The weight coefficient may vary depending on the results of the expert survey.

3. Calculation of the index of the information potential indicator of energy enterprises with the weight coefficient calculated in accordance with (5)

$$P_i = q_{ip} \cdot P_{Ni}, \quad (5)$$

where P_i is the index of the information potential of energy enterprises with the weight coefficient;

P_{Ni} is the normalized indicator of the information potential of energy enterprises.

4. Calculation of the integral index of the information potential of energy enterprises according to (6)

$$\sum P_{\inf p} = q_1 \cdot P_{avt} + q_2 \cdot P_{\inf} + q_3 \cdot P_{fax} + q_4 \cdot P_{inb} + q_5 \cdot P_{zs}, \quad (6)$$

where P_{avt}, P_{inf}, P_{fax}, P_{inb}, P_{zs} – values of the corresponding indices of the information potential of energy enterprises with the inclusion of a weight coefficient;

q_1, q_2, q_3, q_4, q_5 are the weight coefficients of the corresponding indicators (P_{avt}, P_{inf}, P_{fax}, P_{inb}, P_{zs}) of the information potential of energy enterprises.

5. By the expert method, based on the decisions of specialists and the requirements of industry and standards of the International Electrotechnical Commission [18], a scale for assessing the integral index of the information potential of enterprises is proposed (Table 1).

At this stage, it is important to:

– compare the obtained integral indices between enterprises to understand the level of information potential of each enterprise;

– analyze how changes in indicators (for example, increased investment in information technologies) affect the overall index;

– assess how a high or low level of information potential affects various aspects of the enterprise's activities (financial results, quality of services, competitiveness, etc.).

Comparison with other energy enterprises makes it possible to understand where enterprises are in comparison with competitors or other enterprises in the industry; to assess the competitive advantages of enterprises with high information potential.

Table 1

Scale for assessing the integral index of the level of information potential of energy enterprises

No. of entry	The value of the integral index of the indicator of the level of information potential ($\sum P_{infp}$)	Level of information potential	Score
1	0.80-1.00	Very high	Norm
2	0.60-0.79	High	Norm
3	0.40-0.59	Average	Conditional norm
4	0.20-0.39	Low	Abnormal
5	0.00-0.19	Very low	Abnormal

5. 2. Verification of the methodology using real data on energy enterprises

The level of information potential of Zaporizhzhia (ZTES), Burshtynska (BTES), and Vuglehirska (VTES) power plants was assessed during 2012–2024. The initial data and their normalization, which was carried out on the basis of expert analysis of the level of information potential, for each power plant during 2012–2024, are given in Table 2.

Next, the expert method was used to determine the weighting coefficient for each indicator of information potential:

– q_1=0.25 for the automation indicator (P_{avt});

– q_2=0.20 for the IT infrastructure indicator (P_{inf});

– q_3=0.15 for the IT specialists per 100 people indicator (P_{fax});

– q_4=0.20 for the information security indicator (P_{inb})

– q_5=0.20 for the digital systems indicator (P_{zs}).

Calculation of indices for the indicators of information potential of energy enterprises with taking into account the weight coefficient, carried out in accordance with formulas (1) to (6) for 2012–2024, and the results obtained are summarized in Table 3.

Based on our calculations of information potential indicators (Table 3), a comprehensive analysis of the level of information potential was conducted using expert assessment methods. The results of the expert assessment show that the highest level of information potential of energy enterprises was observed in the period from 2012 to the end of 2013, on the assessment scale 1, stably remaining at the level of:

– 0.79 arbitrary units for ZTES;

– 0.6165 arbitrary units for VTES;

– 0.8975 arbitrary units for BTS.

Such stability was ensured by systematic measures to support and develop the information potential of enterprises under conditions of digital coherence, in accordance with regulated standards and procedures.

A significant decrease in the level of information potential was recorded at the beginning of 2014, which coincided with the beginning of military aggression by the Russian Federation against Ukraine. During 2014–2021, the level of information potential decreased by 0.1910 arbitrary units for ZTES; by

0.2255 arbitrary units for VTES; by 0.2185 arbitrary units for BTS. This deterioration was due to both the destabilization of the general security situation and the emergence of new cyber threats aimed at disrupting the functioning of automated control systems of technological processes of power plants.

In the period from February 2022 to the end of 2023, there is a sharp and critical decrease in the level of information potential from 0.5790 to 0.3710 arbitrary units for ZTES; from 0.3910 to 0.2225 arbitrary units for VTES; from 0.6790 to 0.5260 arbitrary units for BTS.

Table 2

Initial and normative data on the information potential of power plants over 2012–2024

Name of the indicator of information potential	Real/normalized parameter of the indicator of information potential			Weight	Year
	ZTES	VTES	BTES		
P_{avt} – automation indicator, (arbitrary units)	70/0.7	60/0.6	75/0.7	0.25	2012–2013
	60/0.6	50/0.5	70/0.7	0.25	2014–2021
	50/0.5	40/0.4	60/0.6	0.25	2022–2023
	30/0.3	25/0.25	40/0.4	0.25	2024
P_{inf} – IT infrastructure indicator, (arbitrary units)	1/1	0.8/0.8	1/1	0.20	2012–2013
	0.8/08	0.5/0.5	0.9/0.9	0.20	2014–2021
	0.5/0.3	0.3/0.3	0.7/0.7	0.20	2022–2023
	0.7/0.7	0.5/0.5	0.6/0.6	0.20	2024
P_{fax} – indicator of IT specialists per 100 people, (arbitrary units)	10/0.5	7/0.35	12/1	0.15	2012–2013
	8/0.4	6/0.3	10/0.5	0.15	2014–2021
	5/0.25	3/0.15	8/0.4	0.15	2022–2023
	5/0.25	4/0.12	6/0.3	0.15	2024
P_{inb} – information security indicator, (arbitrary units)	7/0.7	6/0.6	8/0.8	0.20	2012–2013
	5/0.5	4/0.4	7/0.7	0.20	2014–2021
	4/0.4	3/0.3	6/0.6	0.20	2022–2023
	5/0.5	4/0.4	6/0.6	0.20	2024
P_{zs} – indicator digital systems, (arbitrary units)	3/1.0	2/0.666	3/1.0	0.20	2012–2013
	2/0.666	1/0.333	2/0.666	0.20	2014–21
	1/0.333	0/0	1/0.333	0.20	2022–2023
	2/0.666	1/0.333	2/0.666	0.20	2024

Table 3

Final results from calculating the indicators of information potential of power plants over 2012–2024

Indicator of information potential	Power plant			Year
	ZTES	VTES	BTES	
P_{avt} – automation indicator, (arbitrary units)	0.175	0.15	0.1875	2012–2013
	0.125	0.1	0.15	2014–2021
	0.0875	0.08	0.14	2022–2023
	0.07	0.0625	0.12	2024
P_{inf} – IT infrastructure indicator, (arbitrary units)	0.2	0.16	0.2	2012–2013
	0.16	0.1	0.18	2014–2021
	0.1	0.06	0.14	2022–2023
	0.096	0.052	0.104	2024
P_{fax} – indicator of IT specialists per 100 people, (arbitrary units)	0.075	0.0525	0.15	2012–2013
	0.06	0.045	0.075	2014–2021
	0.0375	0.0225	0.06	2022–2023
	0.03	0.018	0.045	2024
P_{inb} – information security indicator, (arbitrary units)	0.14	0.12	0.16	2012–2013
	0.1	0.08	0.14	2014–2021
	0.08	0.06	0.12	2022
	0.072	0.052	0.1	2024
P_{zs} – indicator digital systems, (arbitrary units)	0.2	0.134	0.2	2012–2013
	0.134	0.066	0.134	2014–21
	0.066	0	0.066	2022–2023
	0.054	0	0.054	2024
P_{Σ} – integral indicator of information potential, (arbitrary units)	0.7900 (norm, high)	0.6165 (norm, high)	0.8975 (norm, very high)	2012–2013
	0.5790 (conditional norm, average)	0.3910 (abnormal, low)	0.6790 (norm, high)	2014–2021
	0.3710 (abnormal, low)	0.2225 (abnormal, low)	0.5260 (conditional norm, average)	2022–2023
	0.3220 (abnormal, low)	0.1845 (abnormal, very low)	0.4230 (conditional norm, average)	2024

This drop is associated with the beginning of military actions by Russia, which caused serious economic and technological difficulties. Additionally, this drop could have been caused by the following factors:

– the impact of global crises, in particular military aggression and economic instability;

– reduction or cancellation of investments in digital technologies due to military actions and economic difficulties;

– possible changes in policy or legislation that limited the possibilities for the implementation of new information technologies;

– there may have been major incidents or a series of incidents at the station that led to a temporary decrease in the effectiveness of digital technologies.

A further decline in the level of information potential during 2023 and 2024 is associated with the duration of military actions by Russia, which caused significant economic and technological difficulties:

– technological obsolescence or lack of updates due to limited information resources and investments under wartime conditions;

– reduced investment in innovation due to the economic crisis caused by the war;

– problems with technical maintenance and support of new technologies due to the complex information security situation and limited access to the necessary information resources.

This decline in the level of information potential may also be a consequence of a lag in the development of new digital technologies or a change in the company's priorities in the context of military operations.

Fig. 2 shows a diagram of the dynamics of changes in the integral indicators of the information potential of the power plant during 2012–2024. The diagram helps track the dynamics of changes in all integral indicators of the information potential of the power plant during 2012–2024 and identify critical points for timely decision-making on eliminating information potential risks.

During periods of decline, as in 2014, 2022–2024, a decrease in information potential indicators leads to a decrease in the level of the integral indicator of the information potential, which indicates a decrease in efficiency and innovative potential.

In addition, this drop in the integral indicators of the information potential significantly exceeds the threshold values determined by the requirements for regulated standards and procedures, which indicates a significant deterioration in the situation.

Such dynamics are directly related to the beginning of full-scale military operations by the Russian army, as well as damage to the software and hardware complexes of automated systems, which created unprecedented threats to its information potential at the power plant.

The results of the expert assessment clearly demonstrate the cause-and-effect relationships between the level of information potential and external factors, in particular military aggression by the Russian army.

This approach allows for a deeper understanding of the nature of the identified risks and to identify ways to overcome them to ensure the proper level of information potential of energy enterprises.

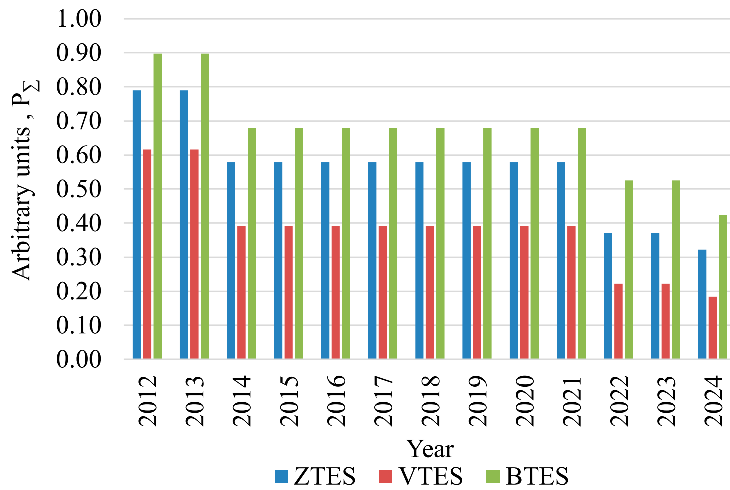

Fig. 2. Diagram of the dynamics of changes in the integrated indicators of the information potential of the power plant during 2012–2024

6. Discussion of results related to devising a methodology for assessing the level of information potential of energy enterprises

The proposed methodology for assessing the level of information potential of energy enterprises solves a number of key problems that arise when using existing approaches to assessing information potential under conditions of digital coherence. The methodology is an important tool for managing the information potential of energy enterprises, but it is shown that its effectiveness depends on the accuracy of data, the level of personnel training and the availability of information resources for implementation.

Unlike [19, 20], in which information components and their indicators are not taken into account, the information potential of an energy enterprise is considered as an integral complex, including information, technical, organizational, and human resources. This allows for a more detailed study of the nature of the identified risks and the definition of effective measures to eliminate them in order to guarantee the appropriate level of information potential of energy enterprises.

The stages of component selection take into account their interaction and integration into the overall information potential management system of an energy enterprise. Components such as the level of automation and IT infrastructure contribute to reducing costs and increasing productivity. Scientific research confirms that process automation reduces the number of errors and speeds up task completion. In the context of digital transformation, the protection of information resources is critically important. The selection of components that ensure information security minimizes the risks of cyberattacks and data loss. The level of personnel determines the ability of the enterprise to effectively use information potential. Investments in training and development of personnel are key to maintaining information potential.

Based on the results of calculating information potential indicators (Table 3), a diagram (Fig. 2) was constructed for the dynamics of changes in the potential of energy enterprises during 2012–2024.

The diagram (Fig. 2) for the dynamics of changes in the integral indicators of the information potential of energy enterprises for the period 2012–2024 demonstrates how the level of information potential changed over time, which makes it possible to assess the overall dynamics of development. Also, the diagram (Fig. 2) shows periods when the indicators significantly decreased or increased, which may be due to external factors, such as economic crises, technological changes, or the impact of hostilities. Based on the dynamics of past years, it is possible to make forecasts regarding the future development of the information potential of energy enterprises. In addition, the diagram helps determine which aspects of the information potential require additional attention and develop strategies for their improvement.

The methodology for practical application may require significant investments in new technologies, the introduction of new standards and processes, which may be economically unaffordable for energy enterprises.

The practical application of the methodology for assessing the level of information potential of energy enterprises may require significant effort, time, and financial resources. In addition, under complex or unstable conditions of the information environment, problems may arise with the accuracy and completeness of the source data, which affects the quality of assessing the level of information potential of energy enterprises.

Further research will focus on the relationship between the information potential of the enterprise, its architecture, and economic potential. Clustering of enterprises by the level of their information potential and analysis of the results will also be carried out.

7. Conclusions

1. Stages of the methodology for assessing the level of information potential of energy enterprises have been proposed, which is an important tool for assessing and managing the level of information potential of energy enterprises, especially under the conditions of digital coherence. The methodology takes into account the interaction and integration of technical, organizational, information, and personnel resources, which provides a holistic view of the level of information potential of enterprises. The selection of such components as process automation, modernization of IT infrastructure, and increasing the level of information security contribute to the economic efficiency of enterprises. Investments in personnel development support the ability of enterprises to adapt to rapid changes in the digital sphere.

2. The methodology was verified on real data of energy enterprises to assess its effectiveness. Experimental testing of the methodology at enterprises of the electric power system confirmed its effectiveness, practical value, and versatility under the conditions of a real digital environment. The constructed diagram of the dynamics of changes in the integral indicators of IP during 2012–2024 makes it possible to visually assess the dynamics of changes in the indicators of information potential and identify critical points for prompt response to risks. The effectiveness of practical application of the methodology depends on the accuracy of the source data, the availability of resources, and the level of personnel training. Disadvantages, such as the complexity of integration into existing systems or economic constraints, require additional consideration.

Conflicts of interest

The authors declare that they have no conflicts of interest in relation to the current study, including financial, personal, authorship, or any other, that could affect the study, as well as the results reported in this paper.

Funding

The study was conducted without financial support.

Data availability

All data are available, either in numerical or graphical form, in the main text of the manuscript.

Use of artificial intelligence

The authors confirm that they did not use artificial intelligence technologies when creating the current work.

References

1. Walter, L., Denter, N. M., Kebel, J. (2022). A review on digitalization trends in patent information databases and interrogation tools. World Patent Information, 69, 102107. https://doi.org/10.1016/j.wpi.2022.102107
2. Berdik, D., Otoum, S., Schmidt, N., Porter, D., Jararweh, Y. (2021). A Survey on Blockchain for Information Systems Management and Security. Information Processing & Management, 58 (1), 102397. https://doi.org/10.1016/j.ipm.2020.102397
3. Maddikunta, P. K. R., Pham, Q.-V., B, P., Deepa, N., Dev, K., Gadekallu, T. R., Ruby, R., Liyanage, M. (2022). Industry 5.0: A survey on enabling technologies and potential applications. Journal of Industrial Information Integration, 26, 100257. https://doi.org/10.1016/j.jii.2021.100257
4. Hughes, L., Dwivedi, Y. K., Misra, S. K., Rana, N. P., Raghavan, V., Akella, V. (2019). Blockchain research, practice and policy: Applications, benefits, limitations, emerging research themes and research agenda. International Journal of Information Management, 49, 114–129. https://doi.org/10.1016/j.ijinfomgt.2019.02.005
5. Fedushko, S., Benova, E. (2019). Semantic analysis for information and communication threats detection of online service users. Procedia Computer Science, 160, 254–259. https://doi.org/10.1016/j.procs.2019.09.465
6. Gunduz, M. Z., Das, R. (2020). Cyber-security on smart grid: Threats and potential solutions. Computer Networks, 169, 107094. https://doi.org/10.1016/j.comnet.2019.107094
7. Tolah, A., Furnell, S. M., Papadaki, M. (2021). An empirical analysis of the information security culture key factors framework. Computers & Security, 108, 102354. https://doi.org/10.1016/j.cose.2021.102354

8. Andersson, A., Hedström, K., Karlsson, F. (2022). Standardizing information security – a structurational analysis. Information & Management, 59(3), 103623. https://doi.org/10.1016/j.im.2022.103623
9. Hadlington, L., Binder, J., Stanulewicz, N. (2021). Exploring role of moral disengagement and counterproductive work behaviours in information security awareness. Computers in Human Behavior, 114, 106557. https://doi.org/10.1016/j.chb.2020.106557
10. Xu, L. D., Duan, L. (2018). Big data for cyber physical systems in industry 4.0: a survey. Enterprise Information Systems, 13 (2), 148–169. https://doi.org/10.1080/17517575.2018.1442934
11. Nishant, R., Kennedy, M., Corbett, J. (2020). Artificial intelligence for sustainability: Challenges, opportunities, and a research agenda. International Journal of Information Management, 53, 102104. https://doi.org/10.1016/j.ijinfomgt.2020.102104
12. Diachkov, D. V. (2014). Estimation of information potential of industrial enterprises. Ekonomika. Menedzhment. Pidpryiemnytstvo, 26 (1), 75–84. Available at: http://nbuv.gov.ua/UJRN/ecmepi_2014_26(1)__11
13. Diachkov, D. V. (2012). Metodychni pidkhody do otsinky informatsiynoho potentsialu pidpryiemstva. Naukovyi visnyk Poltavskoho universytetu ekonomiky i torhivl, 4 (55), 131–135. Available at: http://nbuv.gov.ua/UJRN/Nvpusk_2012_4_27
14. Prokhorova, V., Protsenko, V., Bezuglaya, Y., Us, J. (2018). The optimization algorithm for the directions of influence of risk factors on the system that manages the potential of machine-building enterprises. Eastern-European Journal of Enterprise Technologies, 4 (1 (94)), 6–13. https://doi.org/10.15587/1729-4061.2018.139513
15. Shibaeva, N., Baban, T., Prokhorova, V., Karlova, O., Girzheva, O., Krutko, M. (2019). Methodological bases of estimating the efficiency of organizational and economic mechanism of regulatory policy in agriculture. Global Journal of Environmental Science and Management, 5, 160–171. https://doi.org/10.22034/gjesm.2019.05.SI.18
16. Babenko, V., Baksalova, O., Prokhorova, V., Dykan, V., Ovchynnikova, V., Chobitok, V. (2021). Information And Consulting Service Using In The Organization Of Personnel Management. Studies of Applied Economics, 38 (4). https://doi.org/10.25115/eea.v38i4.3999
17. Iarmosh, O., Prokhorova, V., Shcherbyna, I., Kashaba, O., Slastianykova, K. (2021). Innovativeness of the creative economy as a component of the Ukrainian and the world sustainable development strategy. IOP Conference Series: Earth and Environmental Science, 628 (1), 012035. https://doi.org/10.1088/1755-1315/628/1/012035
18. MEK 62443-2-1. Promyslovi komunikatsiyni merezhi – Informatsiyna bezpeka merezhi ta systemy – Chastyna 2-1: Stvorennia prohramy informatsiynoi bezpeky systemy promyslovoi avtomatyzatsiyi. Available at: https://tk185.appau.org.ua/downloads/IEC_62443_2_1_ukr_draft.pdf
19. Prokhorova, V., Budanov, M., Budanov, P., Zaitseva, A., Slastianykova, A. (2025). Devising a comprehensive methodology for estimating the economic efficiency of implementing an investment project for ensuring energy security of enterprises: organizational-economic aspect. Eastern-European Journal of Enterprise Technologies, 1 (13 (133)), 59–68. https://doi.org/10.15587/1729-4061.2025.321965
20. Prokhorova, V., Budanov, O., Budanov, P., Slastianykova, K. (2025). Comprehensive methodology for estimating information safety at enterprises of electroenergy system under the conditions of digital coherence. Eastern-European Journal of Enterprise Technologies, 2 (13 (134)), 27–37. https://doi.org/10.15587/1729-4061.2025.327159