The object of this study is the process of assessing the information security of enterprises within an electric power system at the economy's micro-level under the conditions of digital coherence.

The work solves the task to devise a comprehensive and adaptive approach to assessing information security, taking into account modern challenges associated with the integration of digital systems. The main feature is that the methodology enables to analyze the relationships between infrastructure components, taking into account digital coherence, which makes it possible to improve the accuracy of risk assessment and the effectiveness of information security management.

The devised methodology is based on eight interconnected stages, which include the integration of indicators, assessment of the interaction of system components, and monitoring changes in information security indicators in real time. This allows enterprises to respond to threats in a timely manner, minimizing risks.

A computational algorithm has been developed that monitors the dynamics of changes in information security indicators, which contributes to making timely management decisions.

The practical application of the methodology has been justified by scenarios of its integration into the work of energy industry enterprises. Testing at the power unit of the Zaporizhzhia Nuclear Power Plant confirmed its effectiveness, providing an economic effect of about USD 90 thousand. The methodology could be applied at different levels of the economy and adapted to the needs of specific enterprises, including integration into existing monitoring and management systems.

The results demonstrate the uniqueness of the proposed approach due to its complexity, adaptability, and practical significance, which makes the methodology an effective tool for assessing information security in the context of digital coherence

Keywords: energy enterprises, information threats, information risks, indicators of information security, digital coherence, methodology for assessing information security

UDC 658.155:004.42
DOI: 10.15587/1729-4061.2025.327159

COMPREHENSIVE METHODOLOGY FOR ESTIMATING INFORMATION SAFETY AT ENTERPRISES OF ELECTROENERGY SYSTEM UNDER THE CONDITIONS OF DIGITAL COHERENCE

Viktoriia Prokhorova
Doctor of Economic Sciences, Professor*
Oleksandr Budanov
PhD Student*
Svobody sq., 4, Kharkiv, Ukraine, 61022
Pavlo Budanov
Corresponding author
PhD, Associate Professor
Department of Physics, 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 05.02.2025
Received in revised form 25.03.2025
Accepted 15.04.2025
Published 22.04.2025

How to Cite: *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*

1. Introduction

In today's world, power utilities are increasingly integrating digital technologies, which can improve efficiency, but at the same time create new cyber threats. Ensuring reliable information security (IS) is becoming critical to preventing major disruptions in power supply and reducing the risk of loss or theft of sensitive information.

The interaction of numerous digital systems and technologies within a single infrastructure (digital coherence) makes it necessary to implement new methods for assessing the information security of power system enterprises at the macro, meso, and micro levels of the economy. Conventional approaches to information protection, which focus on individual systems, are unable to adequately assess and protect the entire power system at the macro, meso, and micro levels of the economy. Cybercriminals are becoming increasingly resourceful, using the latest technologies to attack power enterprises. The rapid development of technologies and the increase in the number of cyber threats, in particular complex and coordinated attacks, such as viruses, phishing, require new approaches to assessing and protecting information systems. This can lead to significant economic losses, damage to infrastructure or even threats to national security. The relevance of the topic is growing due to the need to devise methods that allow for timely assessment and neutralization of these threats. Many enterprises have numerous and diverse information systems, which requires devising comprehensive assessment methods that take into account the interaction of macro, meso, and micro levels of the economy. The lack of such an integrated methodology can lead to gaps in the assessment of risks and security.

Many existing methodologies for assessing information security do not take into account the complexity and interac-

tion of different levels of information systems in the electric power industry. This creates gaps in the identification of risks and vulnerabilities at the macro, meso, and micro levels of the economy. As digital technologies are constantly evolving, there is a need to devise adaptive assessment methodologies that can take into account changes in the digital environment and provide a timely response to new threats.

Thus, the relevance of the research topic is due to the need to devise an effective comprehensive methodology for assessing the information security of enterprises in the electric power industry in the context of the rapid development of digital technologies and the growing complexity of cyber threats. This is important for taking into account the interaction of digital technologies at different levels of the economy and would allow for effective assessment of information security, increasing the level of protection of enterprises in the electric power system in the context of constantly changing threats.

2. Literature review and problem statement

In [1], studies focus only on technical aspects (e.g., vulnerability analysis or technical threats), without taking into account the interaction of different digital systems and the impact of digital coherence. This limits the accuracy and completeness of the assessment of the level and level of information security of energy system enterprises at the macro, meso, and micro levels of the economy.

Given the multi-level nature of energy enterprises, where the macro, meso, and micro levels are interconnected, in [2], these levels are not sufficiently integrated into a single assessment system. This can lead to an incomplete picture of threats and risks that arise due to digital integration at all levels.

In [3], rapid changes in digital technologies and new cyber threats that are constantly emerging are not taken into account. The assessment of information security according to old models is unable to take into account rapid changes in the technological environment, which reduces the effectiveness of enterprise protection.

In works [4, 5], insufficient attention is paid to the influence of the human factor on the level of security, in particular user errors, insufficient qualification of personnel or the lack of an appropriate security culture. However, as noted in [6], these factors can significantly affect the overall level of information security of the enterprise.

In [7], modern regulatory and legal requirements for information security are not taken into account, which complicates the application of the results in practice. Lack of compliance with the requirements of national or international standards can lead to non-compliance with real security requirements.

In [8], ensuring the level of information security is limited to technological aspects. The studies focus on protecting networks, software, or data storage systems, and do not consider the importance of organizational and procedural aspects of security, which may be no less important for ensuring comprehensive protection.

In [9], the study focuses on the current level of information security without properly predicting future threats and trends in the development of digital technologies, which may limit their usefulness for strategic planning and development.

Given that in the context of digital coherence, different systems and platforms are integrated with each other, in [10], a study was conducted that does not take into account the effects of this integration, which may lead to an incomplete assessment of vulnerabilities and risks arising from the interaction of different components.

In [11], insufficient emphasis is on intersectoral cooperation. Lack of attention to the importance of cooperation between enterprises, government agencies, and other ecosystem participants that have common interests in ensuring the information security of critical infrastructures. This can lead to gaps in cyber threat response systems.

In works [12, 13], the use of modern technologies and tools is limited. Modern tools for information security assessment, such as big data analytics, artificial intelligence, or machine learning, which can significantly improve the accuracy and speed of enterprise information security assessment, are not sufficiently used.

These shortcomings limit the effectiveness of conventional approaches to assessing IBS and indicate the need to develop more comprehensive, integrated, and adaptive assessment methods that can take into account modern challenges in the context of digital transformation.

Thus, our review of the literature [1–13] demonstrates that there is part of the unresolved problem of assessing the level and level of information security of enterprises of the electric power system at the macro, meso, and micro levels of the economy, namely:

– insufficient integration of different levels of information security assessment (for example, the relationship between macro, meso, and micro levels is not taken into account, which leads to a fragmented assessment of IS level);

– limited consideration of digital coherence (for example, existing assessment methods do not sufficiently take into account the integration and interaction of digital systems at different levels, which is important in the context of modern digital transformation of enterprises);

– underestimation of organizational and procedural aspects of IS (for example, most studies focus on technical aspects of IS, not paying sufficient attention to organizational and procedural measures, which are no less important for ensuring comprehensive protection of information resources);

– lack of adaptation to new cyber threats (for example, conventional IS assessment methods are unable to adequately respond to new cyber threats and technological changes, which requires the development of more flexible and dynamic methods to adapt to a rapidly changing environment);

– insufficient attention to the human factor (for example, many studies do not take into account the importance of the human factor in information security, in particular user errors, insufficient staff qualifications or the lack of a proper IS culture, which are significant sources of potential threats);

– inconsistency with current regulatory requirements: Some studies do not take into account modern regulatory and legal acts regulating information security at the national and international levels, which reduces the practical value of the proposed methods for real-world application.

These problems indicate the need to devise new, more comprehensive approaches to assessing the information security of energy system enterprises that take into account digital integration and all levels of the economy, as well as adapt to the latest cybersecurity challenges.

3. The aim and objectives of the study

The purpose of our study is to devise a comprehensive methodology for assessing the information security of enter-

prises of the electric power system under conditions of digital coherence. This will make it possible to effectively assess and manage the risks of information security of enterprises of the electric power system at the macro, meso, and micro levels of the economy, taking into account the interaction of digital technologies and systems.

To achieve the goal, the following tasks were set:

– to define stages of a comprehensive methodology for assessing information security, which allows assessing the level of IS of enterprises at all levels – from individual components of information systems to strategic decisions at the level of the electric power industry;

– to develop a computational algorithm that will ensure accurate calculation of information security indicators, taking into account the dynamics of changes in risks, threat indicators and their interrelationships at different levels of management;

– to carry out experimental testing of the comprehensive methodology at enterprises of the electric power system and to investigate its effectiveness in a real digital environment, confirming its practical value and universality.

4. The study materials and methods

The object of our study is the process of assessing the information security of enterprises of the electric power system under the conditions of digital coherence. This includes the analysis and provision of protection of information resources, technologies, and processes used within these enterprises.

The study focuses on the identification, analysis, and management of information security risks, as well as on the development of methods that allow for the effective assessment and provision of protection of information systems of enterprises of the electric power industry under the conditions of intensive digitalization and integration of technologies.

The hypothesis of the study assumes that devising a comprehensive methodology for assessing the information security of enterprises of the electric power system under the conditions of digital coherence could significantly improve the efficiency of IS management due to the following [14–16]:

– it integrates different levels of assessment (macro, meso, micro level), taking into account the specificity of enterprises of the electric power industry and the interaction of digital technologies at each level;

– it takes into account digital coherence, which ensures the integration and interaction of information systems, technologies, and processes, which allows for a more accurate assessment and forecast of risks and threats in a constantly changing digital environment;

– it integrates quantitative and qualitative indicators to assess the level of information security, which allows for a more comprehensive and accurate analysis, as well as promptly adapting IS measures to new threats and requirements;

– it ensures adaptability and efficiency of real-time information security assessment, which allows enterprises to quickly respond to cyber threats and timely adjust IS strategies in the context of digital transformation.

Thus, the hypothesis suggests that the devised comprehensive methodology would improve the ability of energy industry enterprises to effectively manage information security risks and reduce vulnerabilities associated with the integration of digital technologies.

Various methods are used to assess the level of information security of enterprises, which have scientific justifications and practical application. Here are the main ones:

1. Expert assessment method. This is a method in which information security is assessed through the opinions of experts in the field of information technology and information security. Experts assess various aspects of enterprise security, for example, based on an assessment of existing threats and vulnerabilities, the level of protection of information systems. The practical application is that information security is assessed without the need for technical research, but only through the analysis of expert opinion.

2. Risk analysis method. This method involves identifying and assessing risks that may affect the security of enterprise information systems. It includes an analysis of vulnerabilities, threats, the likelihood of their occurrence and possible consequences. The practical application is to devise strategies and measures to minimize risks and reduce the likelihood of threats.

3. The method of monitoring and auditing information security involves regular verification of IS systems and processes through audit checks and automated monitoring. The assessment is carried out on the basis of collected data on user activity, unauthorized access attempts, software vulnerabilities and other factors. The practical application is to maintain the security system at an up-to-date level and to identify new threats.

These methods provide a comprehensive approach to assessing the level of information security of the enterprise, making it possible not only to identify weaknesses but also actively eliminate them.

5. Results of devising a comprehensive methodology for assessing the information security of enterprises in the context of digital coherence

5. 1. Defining stages of the methodology for assessing the information security of enterprises in the context of digital coherence.

Devising a comprehensive methodology for assessing the information security of enterprises in the context of digital coherence includes several stages (Fig. 1), each of which has its specific characteristics:

Stage No. 1 – defining the goals, tasks, and objects of assessing the information security of enterprises in the context of digital coherence:

– objectives of information security assessment;

– tasks of information security assessment;

– objects of information security assessment.

Stage No. 2 – identification and analysis of external and internal threats and risks that may affect the information security of enterprises. The purpose of the stage: Identification and assessment of possible threats and risks that may affect the information security of an enterprise under the conditions of digital coherence, in order to respond in a timely manner and minimize their impact:

– identification of external threats;

– identification of internal threats to the information environment;

– analysis of information security risks;

– methods of information security analysis.

At this stage, it is important to carefully study both external and internal threats to information security, as well as assess possible risks for the enterprise. This makes it possible to form an understanding of which aspects of information

security require the most attention and resources to ensure an adequate level of protection.

Stage No. 3 – defining criteria for assessing the information security of enterprises, which make it possible to measure the effectiveness of the protection measures taken and determine the level of vulnerability of systems. The main key criteria for assessing information security under the conditions of digital coherence:

– confidentiality of information;
– information integrity;
– information availability;
– monitoring and auditing;
– risk management;
– human factors;
– technical level of protection.

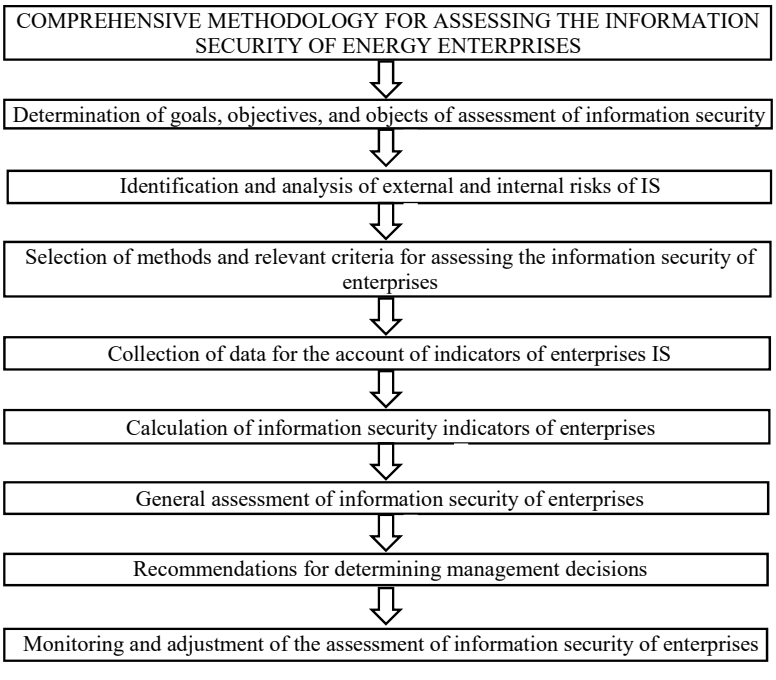

Fig. 1. Flowchart of the stages of the enterprise information security assessment methodology

Stage No. 4 – collection and systematization of data necessary for calculations and analysis of criteria and parameters of information security of the enterprise, which makes it possible to ensure the objectivity of the assessment and the accuracy of the decisions made.

The main sources of data for the assessment of information security:

– technical data;
– organizational data;
– physical data;
– information security incidents;
– technical and external audits.

Data collection is a critical stage for assessing the level of information security of the enterprise under the conditions of digital coherence. This makes it possible to form an objective picture of the current level of security, identify vulnerabilities and determine which aspects need improvement. The accuracy and systematicity of data collection is the basis for further calculations and a correct assessment of the level of information security under the conditions of digital coherence.

Stage No. 5 – calculation of indicators of information security of enterprises. The purpose of the stage: assessment of the level of information security of the enterprise through the calculation of key indicators that make it possible to objectively measure the effectiveness of security systems and identify weaknesses in existing protection measures. The main indicators for calculating information security:

– information security index;
– level of information security risk of enterprises;
– information recovery time;
– level of information availability;
– information confidentiality coefficient;
– information integrity coefficient;
– number of information security incidents;
– information security costs.

Calculating information security indicators is a necessary step to assess the effectiveness of existing protection measures. This makes it possible to understand which aspects need improvement, as well as make informed decisions to reduce risks and increase the level of enterprise IS in the context of digital coherence.

Stage No. 6 – general assessment of enterprise information security based on calculated indicators and analysis of collected data. This stage makes it possible to formulate a final assessment that reflects the level of enterprise information security and provides a basis for further actions to improve it.

The main methods of general assessment of information security:

– comprehensive assessment method;
– scoring system method;
– information security rating.

A general assessment of enterprise information security is an important step to identify weaknesses in the protection system and determine the effectiveness of implemented security measures. This stage helps draw a clear picture of the level of security at the enterprise and determine priorities for further actions to improve security.

Stage No. 7 – determining management decisions to improve and optimize the level of information security of the enterprise, in particular, implementing effective measures that reduce risks and improve information protection.

Management decisions to optimize information security include:

– improving information security risk management measures;
– developing a disaster recovery plan;
– auditing and monitoring;
– reviewing the organizational security structure (for example, reviewing roles and responsibilities in the organization) to determine whether there is a need to expand the security team, improve coordination between departments, or optimize the security management structure;
– determining priorities for implementing changes.

Stage No. 8 – continuous monitoring and analysis of the enterprise's IS indicators to identify new threats, changes in the information environment, and timely adjustments to the IS assessment methodology.

Continuous monitoring of information security indicators is a key component for maintaining a stable and effective level of IS at the enterprise under conditions of digital coherence.

To ensure continuous monitoring of information security indicators under conditions of digital coherence, it is necessary to:

– determine indicators for monitoring information security indicators;

– technical means of monitoring;

– analyze monitoring results;

– make adjustments to the information security assessment methodology;

– adapt to changes in the energy enterprise's environment;

– improve response strategies;

– regularly test the security assessment methodology;

– analyze changes in the technological and legislative environment.

Continuous monitoring and analysis of information security indicators make it possible to timely identify new threats and promptly make adjustments to the enterprise's IS assessment methodology under conditions of digital coherence. This is a necessary condition for ensuring effective protection against attackers and maintaining a high level of information security, especially in the face of constant changes in the technological and legislative environment, in particular for energy companies.

Thus, each stage of the methodology not only logically follows from the previous one but also creates the basis for the next, forming a single sequence of actions that ensures the systematic nature of the process. Defining goals is the starting point that outlines the framework of the study and determines the priorities that must be achieved. At this stage, strategic guidelines are formed, which become criteria for further analysis.

Threat identification allows for a deeper understanding of possible risks and vulnerabilities in the system, in order to identify factors that may negatively affect the achievement of the set goals. This stage creates an information base for devising effective measures to counter threats.

The formation of criteria is an important stage, as it provides structuring of the process, defines clear parameters and standards by which the assessment is carried out. This allows for comparison of various aspects of the studied processes and objects, ensuring objectivity and transparency of the assessment.

The calculation of indicators provides a quantitative basis for assessment, which enhances the validity of the conclusions. The use of mathematical, statistical, or other quantitative methods makes it possible not only to obtain objective data but also compare them in dynamics, to identify trends and patterns.

Monitoring plays an important role in ensuring the dynamic improvement and relevance of the methodology. Regular observation and analysis of the results make it possible to timely detect changes in conditions or parameters, make necessary adjustments and ensure constant adaptation of the process to new challenges.

A systematic approach in this context guarantees not only the accuracy and efficiency of the process but also its continuous adaptation to changes in the information environment. This ensures the stability and reliability of the methodology, as well as its ability to quickly respond to new challenges and opportunities.

The task was to devise a structured approach to analyzing the state of information security in the context of digital coherence. Therefore, the stages defined confirm that the proposed methodology makes it possible to systematize the assessment of threats and risks, form criteria for analysis and implement mechanisms for monitoring information security. Thus, the result is the creation of a basis for a systematic analysis of information security with a clear consideration of the specificity of energy enterprises.

5. 2. Developing a computational algorithm for calculating information security indicators of energy enterprises

To implement a comprehensive methodology for assessing information security to ensure the level of IS of energy enterprises under conditions of digital coherence, an algorithm for calculating IS indicators of energy enterprises is proposed, which combines various aspects of IS (Fig. 2).

The algorithm for calculating information security indicators allows for a comprehensive, systematic, and structured approach to assessing IS, ensuring that all important factors and risks in the field of IS of energy enterprises are taken into account in the context of digital coherence [17].

The algorithm developed for assessing information security has several key features:

– a systematic approach that provides a clear structure for assessing information security, which helps to avoid omissions in the process;

– vulnerability identification (for example, thanks to the threat and vulnerability identification stage, an enterprise can identify weaknesses in its systems that can be used by attackers);

– risk assessment (for example, the algorithm makes it possible to assess the probability of threats and potential damage, which helps in prioritizing security measures);

– development of recommendations (for example, based on the identified risks, an organization can devise specific recommendations to improve its information security);

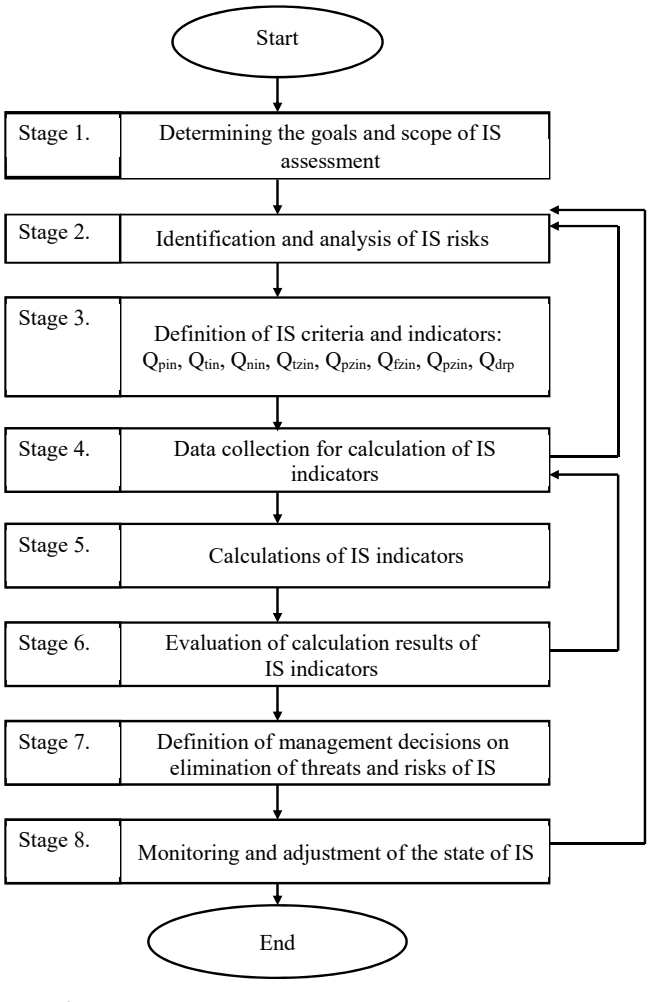

Fig. 2. Flowchart of the algorithm for calculating information security indicators

– documentation (e.g., preparing a report with the results of the assessment ensures transparency and accessibility of information to stakeholders, which can be important for decision-making at the management level of the enterprise);

– monitoring and improvement (e.g., establishing a regular monitoring process allows the organization to adapt to changes in threats and technologies, ensuring that security measures are constantly relevant).

In general, this algorithm is an important tool for information security management, helping organizations protect their data and systems from potential threats.

Adding functionality to the algorithm for monitoring information security indicators, for tracking threats and risks, in real time, is critical for timely decision-making [18].

This algorithm not only optimizes management processes but also provides a systematic approach to analyzing risks and threats that arise in a dynamic information environment.

Integration of this algorithm in software and computing complexes of automated process control systems (ACS) of electricity generation facilities is an important step in increasing the level of information security of electric power enterprises [19].

The task was to develop algorithmic support for quantitative analysis of information security criteria under conditions of digital coherence. The algorithm developed provides high accuracy of calculations, takes into account the specificity of nonlinear processes and allows for rapid assessment of the level of risks. This result confirms the effectiveness of the algorithm as a tool for automated information security analysis.

5. 3. Conducting a study based on the results of practical application of a comprehensive methodology for assessing information security of enterprises

An assessment of the information security at the Zaporizhzhia Nuclear Power Plant (ZNPP) was carried out under conditions of digital coherence. In order to carry out calculations for all information security indicators for the Zaporizhzhia NPP, it is necessary to determine the values for each of the coefficients.

To calculate the IS indicators, which are determined by the expert assessment method on a scale from 0 to 5 points, it is advisable to use a comprehensive set of input data, covering technical, organizational, financial, and regulatory aspects:

– technical condition of equipment (0–5 points);
– staffing (0–5 points);
– financing (0–5 points);
– data access system (0–5 points);
– network protection (0–5 points);
– antivirus software (0–5 points);
– software updates (0–5 points);
– information security budget (0–5 points);
– investments in protection (0–5 points);
– legislation (0–5 points);
– contracts with suppliers (0–5 points);
– experience of technical staff (0–5 points);
– experience of administrative staff (0–5 points);

According to the comprehensive information security assessment methodology, indicators for assessing the information security of the Zaporizhia NPP were selected. This approach allows for a comprehensive assessment of the state of information security, taking into account all important factors that may affect its level.

To this end, a unified calculation of the information security indicators of the Zaporizhia NPP was considered based on the reports by IAEA experts over 2022–2023 (GC(67)/2; GC(68)/2) [20, 21], and a review of their activities for 2024 [22]. These reports contain a detailed analysis of the state of information security, recommendations for eliminating vulnerabilities, and an assessment of the impact of digital threats on the functioning of the Zaporizhia NPP:

1. The information completeness indicator is calculated according to expression (1):

$$Q_{pin} = \frac{I_{in}}{I_{yr}}, \quad (1)$$

where Q_{pin} is the information completeness coefficient;

I_{in} is the amount of information that enters the automated dashboard of the operator of the ZNPP power unit's TP ACS, %;

I_{yr} is the amount of information that is required for the operator of the ZNPP power unit's TP ACS to make a reasoned decision, %.

2. The information accuracy indicator is calculated according to expression (2):

$$Q_{tin} = \frac{I_{rin}}{I_{in}}, \quad (2)$$

where Q_{tin} is the accuracy coefficient of information received by the operator of the ZNPP power unit's TP ACS;

I_{rin} is the volume of relevant information, %.

3. The information reliability indicator is calculated according to expression (3):

$$Q_{nin} = \frac{I_{nd.in}}{I_{\Sigma in}}, \quad (3)$$

where Q_{nin} is the information accuracy coefficient;

I_{rin} is the amount of information provided to the operator of TP ACS at the ZNPP power unit from reliable information sources, %;

$I_{\Sigma in}$ is the total amount of information provided to the operator of TP ACS at the ZNPP power unit, %.

4. The indicator of technical information protection is calculated according to expression (4):

$$Q_{tzin} = I_{nnin} \cdot K_{at}, \quad (4)$$

where Q_{tzin} is the coefficient of technical information protection;

I_{nnin} is the amount of information provided to the operator of TP ACS at a power unit of ZNPP, the disclosure of which may cause negative consequences for the enterprise, units;

K_{at} is the number of cyberattacks that were not prevented, units.

5. The indicator of software information security is calculated according to expression (5):

$$Q_{pzin} = \frac{T_{bf}}{T_{nf}}, \quad (5)$$

where Q_{pzin} – coefficient of software information security;

T_{bf} – time of uninterrupted operation of the information system of TP ACS at the ZNPP power unit, hours;

T_{nf} – normative time of operation of the information system of TP ACS at the ZNPP power unit, hours.

6. The indicator of financial information protection is calculated according to expression (6):

$$Q_{fzin} = \frac{V_{zinr}}{V_{prin}}, \quad (6)$$

where Q_{fzin} – coefficient of financial information protection;

V_{zinr} – costs of information resources protection: program memory and data memory of PLC of TP ACS at the ZNPP power unit, USD;

V_{prin} – costs of information resources acquisition: program memory and data memory of PLC of TP ACS at the ZNPP power unit, USD.

7. The indicator of legal information protection is calculated according to expression (7):

$$Q_{pzin} = \frac{I_{nnin}}{I_{uzin}}, \quad (7)$$

where Q_{pzin} – coefficient of legal protection of information;

I_{nnin} – volume of information provided only to the operator of TP ACS at the ZNPP power unit, the disclosure of which may cause negative consequences for the enterprise, %;

I_{uzin}– total volume of information that is legally protected and provided only to the operator of TP ACS at the ZNPP power unit, the disclosure of which may cause negative consequences for the enterprise, %.

8. The indicator of experience of the operational personnel of TP ACS at the ZNPP power unit is calculated according to expression (8):

$$Q_{dp} = \frac{N_{dp1r}}{N_{\sum dp}}, \quad (8)$$

where Q_{dp} – coefficient of experience of operators of TP ACS power unit at ZNPP who have access to information, the disclosure of which may cause negative consequences for the enterprise, persons;

N_{dp1r} is the number of operational personnel who have worked at ZNPP for more than one year and have access to information, the disclosure of which may cause negative consequences for the enterprise, persons;

$N_{\sum dr}$ – total number of operational personnel of ZNPP who have access to information, the disclosure of which may cause negative consequences for the enterprise, persons.

The final results of calculating the ZNPP information security indicators, performed according to expressions (1) to (8), are shown in the summary Table 1.

Based on the calculations of information security indicators (Table 1) and the plots (Fig. 3) that reflect the dynamics of changes in information security indicators during the 2010–2024 years of operation of the Zaporizhzhia NPP power units, a comprehensive analysis was carried out using expert assessment methods.

The results of the expert assessment show that the highest level of information security at ZNPP was observed in the period from 2010 to the end of 2013, stably maintaining at the level of 5 points on the assessment scale. Such stability was ensured by systematic measures to support and develop information security under conditions of digital coherence, in accordance with regulated standards and procedures.

A significant decrease in the level of information security was recorded at the beginning of 2014, which coincided with the beginning of military aggression by the Russian Federation against Ukraine. During 2014–2018, the level of information security fluctuated between 2.8 and 3.1 points. 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 ZNPP TP ACS.

In the period from the end of 2018 to the beginning of 2022, there was a positive dynamics in the growth of the level of information security from 2.8 to 4.5 points. This trend was due to the implementation of targeted programs aimed at strengthening cybersecurity, in particular, the allocation of financial and economic resources for the modernization and improvement of the software and hardware of TP ACS power units at ZNPP.

However, since February 2022, there has been a sharp and critical decrease in the level of information security from 4.7 to 2.5 points. This drop significantly exceeds the threshold values defined by the IAEA requirements, 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 the seizure of the territory of the ZNPP, which created unprecedented threats to its information security.

The results of the expert assessment clearly demonstrate the cause-and-effect relationships between the level of information security and external factors, in particular military aggression. This approach allows for a deeper understanding of the nature of the identified risks and identifying ways to overcome them to ensure an adequate level of information security.

Fig. 4 shows a histogram of changes in the dynamics of information security indicators of ZNPP during the 2010–2024 years of operation of ZNPP power units.

The histogram helps track the dynamics of changes in all indicators of ZNPP IS in the period from 2010 to 2024 and identify critical points for timely decision-making on the elimination of risks for ZNPP IS.

Statistical processing methods were used to process the data, in particular, calculating the mean, standard deviation, and coefficient of variation. The results obtained were verified by comparison with previous reports presented in the IAEA reports, which increases the reliability of the conclusions and ensures their compliance with established standards.

For effective monitoring of the information environment, it is proposed to use specialized modules of the software and hardware complex of the automated process control system (TP ACS STC). This provides collection, processing, and analysis of data from various sensors installed on power plants (Fig. 5). IS systems within TP ACS STC allow real-time information on the status of IS, detecting deviations from the norm of IS indicators, and sending warnings to the TP ACS operator for prompt response.

Table 1

Final results of calculating the information security indicators of ZNPP during the 2010—2024 years of operation of the ZNPP power units

Year	Q_{pin}	Q_{tin}	Q_{nin}	Q_{tzin}	Q_{pzin}	Q_{fzin}	Q_{pzin}	Q_{drp}
2010	4.8	4.7	4.8	4.9	5.0	4.8	4.8	4.9
2011	4.9	4.9	4.9	5.0	5.0	4.9	4.8	5.0
2012	5.0	5.0	5.0	5.0	5.0	5.0	5.0	5.0
2013	5.0	5.0	5.0	5.0	5.0	5.0	5.0	5.0
2014	3.1	3.0	2.9	3.0	3.0	2.8	3.0	2.9
2015	2.9	3.0	2.8	2.9	3.0	2.7	2.8	2.9
2016	3.0	3.0	2.8	2.9	3.0	3.0	2.9	3.1
2017	3.0	3.0	2.8	3.0	3.0	3.1	3.0	3.2
2018	3.2	3.0	2.8	3.0	3.3	3.1	3.0	3.2
2019	4.2	4.1	4.3	4.5	4.3	4.2	4.3	4.5
2020	4.3	4.2	4.4	4.6	4.4	4.3	4.4	4.6
2021	4.4	4.3	4.5	4.7	4.5	4.4	4.5	4.7
2022	2.9	3.0	2.8	3.2	3.0	2.8	3.0	2.9
2023	2.8	2.9	2.7	3.1	2.7	2.6	3.0	2.8
2024	2.7	2.8	2.5	3.0	2.5	2.5	2.9	2.5

The economic effect of implementing the information security system module in the TP ACS at NPP power unit can only be indirect because it is not a direct source of income but is an auxiliary means for minimizing costs.

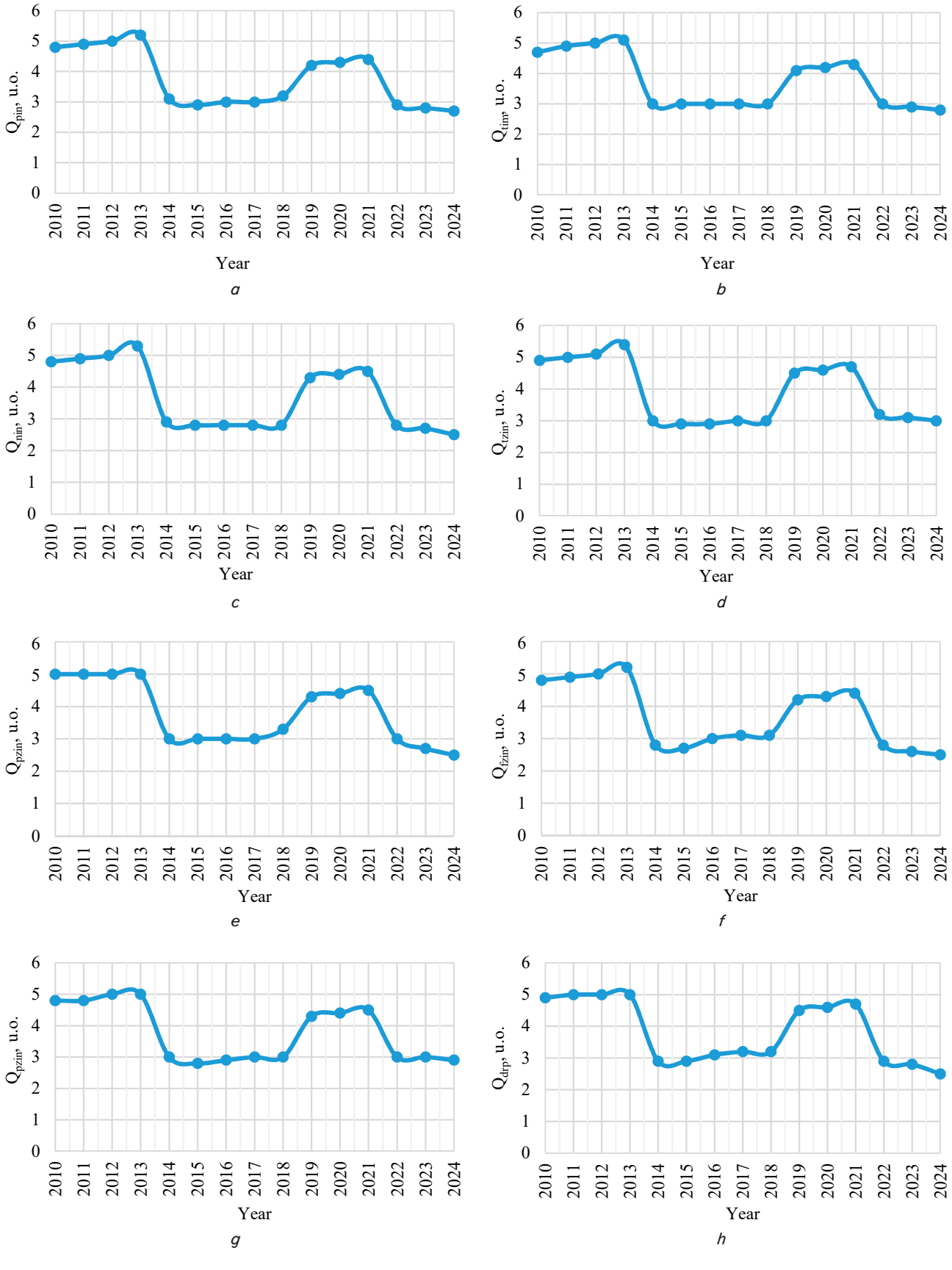

Fig. 3. Plot of changes in the dynamics of enterprise information security indicators: *a* – Q_{pin}; *b* – Q_{tin}; *c* – Q_{nin}; *d* – Q_{tzin}; *e* – Q_{pzin}; *f* – Q_{fzin}; *g* – Q_{pzin}; *h* – Q_{drp}

The cost of implementing one module for detecting information emergency signs, taking into account additional losses, is about USD 10 [19]. It should be noted that the information management system of TP ACS at NPP power unit includes approximately 600 cabinets (depending on the configuration), in which this module must be implemented. Thus, the total cost of implementing the modules of TP ACS information security system for one power unit of the power plant is USD 600×10=6000 (for ZNPP – USD 6000*6=36 thousand).

Considering that due to failures of electrical equipment through untimely detection of threats and risks of the information environment of the technological process, the power plant suffers losses of about USD 45 thousand per year [19]. Therefore, the economic effect of implementing the information security module of TP ACS STC will be about USD 9 thousand.

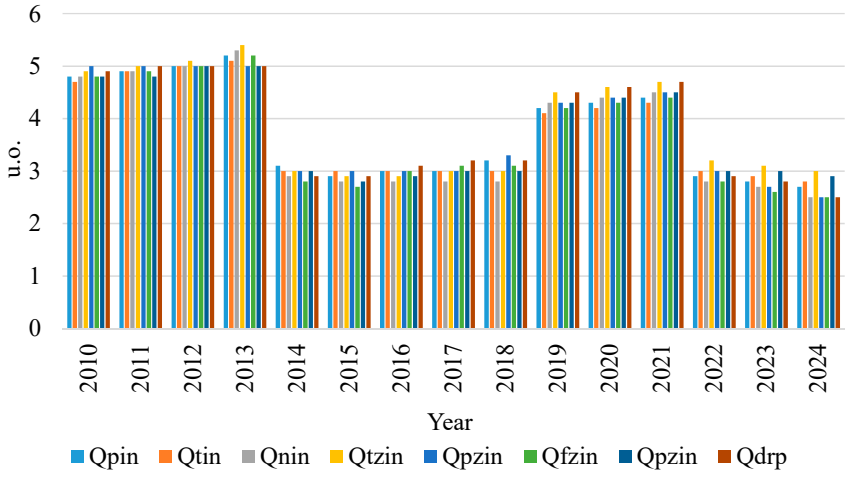

Fig. 4. Histogram of the dynamics of changes in information security indicators of the Zaporizhzhia NPP during the 2010–2024 years of operation of power units

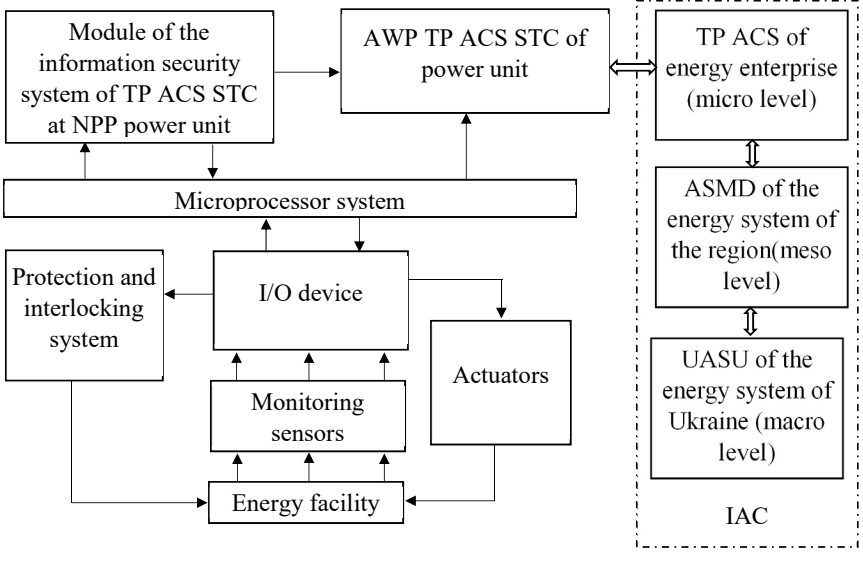

Fig. 5. General structural and functional diagram of the implementation scheme of the information security system module of the software and hardware complex for the automated process control system at the power unit of Zaporizhzhia NPP

To assess the information security of enterprises of the electric power system at the macro and meso levels of the economy, it is proposed to combine ACS STC of the enterprise (power plant) into an integrated automated complex (IAC), as shown in Fig. 5:

– at the meso level, this is ASMD (automated system of management and dispatching of the energy system of the region);

– at the macro level, this is the UASU (unified automated system of the energy system of Ukraine).

The initial data for ASMD and UASU, regarding the assessment of the level of information security at the macro and meso levels, are the results of calculations of integrated indicators of information security, which come from TP ACS of all energy enterprises in the region.

6. Discussion of results based on devising a comprehensive methodology for assessing the level of information security at energy enterprises

The proposed comprehensive methodology for assessing the level of information security (IS) of energy enterprises solves a number of key problems that arise when using existing approaches to assessing IS under conditions of digital coherence. It takes into account a number of factors that have not been sufficiently discussed in previous studies [23, 24], and in particular makes it possible to define the stages indicated in Fig. 1:

– integrate the assessment of IS at all levels of the economy, which provides a holistic view of the state of IS, which reduces fragmentation and ensures a comprehensive approach to assessment;

– focus on digital coherence, which makes it possible to take into account the interactions between various digital components of the enterprise, such as automated control systems, which contributes to a more accurate assessment of IS under conditions of digital coherence;

– ensure the reliability and accuracy of the assessment of not only technical but also organizational and procedural aspects of IS, which is necessary for the sustainable protection of information resources at energy enterprises;

– respond to new cybersecurity challenges, as demonstrated during the assessment of IS at ZNPP, which provides flexibility and dynamism of the methodology, allowing its effective adaptation of protection strategies to new threats;

– integrate measures to train personnel to respond to cyber threats;

– ensure compliance with the requirements of modern regulatory acts and international standards, which increases its practical value for real application at enterprises;

– to take into account digital integration at all levels of the economy and adapt to the latest cybersecurity challenges, providing a reliable and effective tool for managing information security in the context of digital transformation.

To implement a comprehensive methodology for assessing the information security of energy enterprises under

conditions of digital coherence, an algorithm for calculating information security indicators is proposed, the structural block diagram of which is shown in Fig. 2.

This algorithm made it possible to ensure:

– continuous collection and updating of data on information energy security indicators, which allows for a prompt response to changes in the surrounding information environment, such as cyberattacks;

– tracking threats and risks in real time, which is critically important for the processes of managing the information security of energy enterprises;

– integration of this algorithm in the software and computing complexes of the automated process control system of power units of the power plant.

The work has assessed the IS of energy enterprises under conditions of digital coherence, regarding the implementation of the information security system module as part of STC for TP ACS power unit of ZNPP. Based on the results of the calculation of IS indicators (Table 1), which was performed in accordance with expressions (1) to (8), a plot (Fig. 3) of the dynamics of changes in the IS indicators of the enterprise during 2010–2024 was constructed.

Using the diagram of the integrated information security indicator (Fig. 4), it is possible to identify critical points where the IS level under conditions of digital coherence begins to noticeably fall (for example, the point of 2014 and 2022). Such a sharp drop in information security indicators is associated with the beginning of hostilities on the part of Russian Fererederation.

The assessment of the level of IS under conditions of digital coherence may be limited by insufficient accuracy of the initial data, especially under complex or unstable conditions of the information environment of the technological process of power plant units.

During the implementation of the information security module (Fig. 5), problems may arise with the initial calculations, which may lead to false alarms due to unreliable information. These shortcomings may limit the effectiveness and practical application of the proposed methodology under real conditions, and they should be taken into account during its implementation and further improvements.

As disadvantages, the complexity of integrating the proposed algorithm into existing TP ACS of power enterprises can be noted. Real integration into software and computing complexes of TP ACS at enterprises may require significant effort and time.

A comprehensive methodology for practical application may require significant investments in new technologies, the introduction of new standards and processes, which may be economically unaffordable for enterprises, especially under conditions of a limited budget.

This research in the future may focus on training programs for energy company personnel that include skills in responding to cyber threats and implementing cybersecurity best practices. This is possible based on modeling various attack scenarios to train employees in real-world information environments.

7. Conclusions

1. Eight stages of a comprehensive methodology for assessing the IS of energy enterprises have been defined, which allow for the identification and analysis of risks, the definition of criteria, and the calculation of indicators for the objective assessment of IS under the conditions of digital coherence. The developed stages of information security assessment provide not only the systematization of approaches but also form the basis for making management decisions. Detection of cyber threats in the external environment, in real time, significantly reduces the likelihood of serious incidents, which leads to a reduction in risks and financial losses for IS under the conditions of digital coherence.

2. A computational algorithm has been developed that is integrated into the information security assessment system by implementing a comprehensive methodology for assessing the level of enterprise IS in digital coherence. The algorithm adapts to the identified external threats to the information environment, which allows for regular adjustment of management decisions, optimizing enterprise information security management strategies in digital coherence. This not only increases the accuracy of efficiency assessment but also makes the management process more flexible and adaptive. This algorithm allows for early detection of potential problems and implementation of preventive measures, which increases the overall information security of enterprises in digital coherence. The proposed algorithm for adapting to identified external threats is based on dynamic analysis of data obtained from the external information environment and integration into automated enterprise management systems. The adaptation process is implemented through several key mechanisms. The algorithm provides continuous monitoring of external threats, such as cyberattacks, changes in the legislative environment, or man-made factors. Spatial-dynamic monitoring makes it possible to detect new threats at the early stages of their manifestation.

3. As part of investigating the results of the practical application of the comprehensive methodology for assessing the information security of the TP ACS power unit at ZNPP, it was found that the level of IS under conditions of digital coherence directly depends on the frequency of cyberattacks of power unit accidents. For effective monitoring of the information environment, it is proposed to use specialized modules of the software and hardware complex of the automated process control system (TP ACS STC), which provide collection, processing, and analysis of data from various sensors installed on power plants. TP ACSs allow real-time receipt of information about the level of the information security system, detection of deviations from normal values of IS indicators, and sending warnings to the TP ACS operator for prompt response. The implementation of the information security module of TP ACS STC at ZNPP has a significant positive impact on the economic performance of the enterprise. According to calculations, after the implementation of the information security module in the TP ACS STC power unit at ZNPP, the economic effect will be about USD 90 thousand. This indicates a positive financial effect from implementing the module, making the investment worthwhile.

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. Kirilchuk, S., Reutov, V., Nalivaychenko, E., Shevchenko, E., Yaroshenko, A. (2022). Ensuring the security of an automated information system in a regional innovation cluster. Transportation Research Procedia, 63, 607–617. https://doi.org/10.1016/j.trpro.2022.06.054
2. Chang, H. H., Wong, K. H., Lee, H. C. (2022). Peer privacy protection motivation and action on social networking sites: Privacy self-efficacy and information security as moderators. Electronic Commerce Research and Applications, 54, 101176. https://doi.org/10.1016/j.elerap.2022.101176
3. Taherdoost, H. (2022). Cybersecurity vs. Information Security. Procedia Computer Science, 215, 483–487. https://doi.org/10.1016/j.procs.2022.12.050
4. Alraja, M. N., Butt, U. J., Abbod, M. (2023). Information security policies compliance in a global setting: An employee's perspective. Computers & Security, 129, 103208. https://doi.org/10.1016/j.cose.2023.103208
5. 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
6. 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
7. 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
8. Kang, M., Miller, A., Jang, K., Kim, H. (2022). Firm performance and information security technology intellectual property. Technological Forecasting and Social Change, 181, 121735. https://doi.org/10.1016/j.techfore.2022.121735
9. Antunes, M., Maximiano, M., Gomes, R. (2022). A Customizable Web Platform to Manage Standards Compliance of Information Security and Cybersecurity Auditing. Procedia Computer Science, 196, 36–43. https://doi.org/10.1016/j.procs.2021.11.070
10. Ali, S. E. A., Lai, F.-W., Dominic, P. D. D., Brown, N. J., Lowry, P. B. B., Ali, R. F. (2021). Stock market reactions to favorable and unfavorable information security events: A systematic literature review. Computers & Security, 110, 102451. https://doi.org/10.1016/j.cose.2021.102451
11. Gebremeskel, B. K., Jonathan, G. M., Yalew, S. D. (2023). Information Security Challenges During Digital Transformation. Procedia Computer Science, 219, 44–51. https://doi.org/10.1016/j.procs.2023.01.262
12. Tendikov, N., Rzayeva, L., Saoud, B., Shayea, I., Azmi, M. H., Myrzatay, A., Alnakhli, M. (2024). Security Information Event Management data acquisition and analysis methods with machine learning principles. Results in Engineering, 22, 102254. https://doi.org/10.1016/j.rineng.2024.102254
13. Razikin, K., Soewito, B. (2022). Cybersecurity decision support model to designing information technology security system based on risk analysis and cybersecurity framework. Egyptian Informatics Journal, 23 (3), 383–404. https://doi.org/10.1016/j.eij.2022.03.001
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. Budanov, P., Oliinyk, Y., Cherniuk, A., Brovko, K. (2024). Dynamic Fractal Cluster Model of Informational Space Technological Process of Power Station. Information Technology for Education, Science, and Technics, 141–155. https://doi.org/10.1007/978-3-031-71801-4_11
19. Budanov, P., Brovko, K., Cherniuk, A., Vasyuchenko, P., Khomenko, V. (2018). Improving the reliability of informationcontrol systems at power generation facilities based on the fractalcluster theory. Eastern-European Journal of Enterprise Technologies, 2 (9 (92)), 4–12. https://doi.org/10.15587/1729-4061.2018.126427
20. IAEA Annual Report 2022. IAEA. Available at: https://www.iaea.org/sites/default/files/publications/reports/2022/gc67-2.pdf
21. IAEA Annual Report 2023. IAEA. Available at: https://www.iaea.org/sites/default/files/gc/gc68-2.pdf
22. IAEA Year in Review 2024. IAEA. Available at: https://www.iaea.org/newscenter/news/iaea-year-in-review-2024
23. 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
24. Bondar-Pidhurska, O. V., Khomenko, I. I. (2022). Scientific and Methodological Principles of Assessing the Efficiency of the Information Security Process Management of Small and Medium-Sized Businesses: Cybersecurity and Intellectual Property. The Problems of Economy, 2 (52), 108–116. https://doi.org/10.32983/2222-0712-2022-2-108-116