A system for assessing the interdependencies of information system agents in information security risk management using cognitive maps

Yuliia Kostiuk[1,†], Pavlo Skladannyi[1,*,†], Yuliia Samoilenko[2,†], Karyna Khorolska[1,†], Bohdan Bebeshko[1,†] and Volodymyr Sokolov[1,†]

[1] *Borys Grinchenko Kyiv Metropolitan University, Bulvarno-Kudryavska Str., 18/2, Kyiv, 04053, Ukraine*
[2] *National University of Food Technologies, Volodymyrska Str., 68, Kyiv, 01601, Ukraine*

Abstract

To determine the key concepts (information resources, threats, and vulnerabilities) necessary for this study, it is proposed to carry out system modeling of information security risk management processes using the Structured Analysis and Design Technique (SADT). This approach not only facilitates the identification of the relationships and informational content of these processes but also enables the classification of an enterprise's primary information assets, the identification of critical resources, and the determination of the required level of protection. SADT allows for process modeling and the establishment of relationships between information resources, threats, and vulnerabilities, thereby enhancing the identification of system vulnerabilities and enabling more effective planning of protective measures. Information security risk management is an essential component of ensuring the sustainability and continuity of an enterprise's business processes. In the face of a rapidly changing technological environment and a growing number of cyber threats, prioritizing the protection of information resources becomes imperative. This process typically involves several stages, including identifying and assessing resources, identifying potential threats, conducting comprehensive risk analyses, and implementing appropriate measures to minimize or eliminate risks. However, to ensure accurate risk assessments, it is crucial not only to understand individual assets but also to account for their interdependencies. Since each resource may be critical to others within the system, studies that consider these dependencies in the context of information security risk management remain limited. The risk assessment methodology utilizing Fuzzy Cognitive Maps (FCM) offers a means to systematize risk factors for deeper resilience analysis while reducing risks through effective countermeasures. Incorporating the core security attributes—confidentiality, integrity, and availability—enables precise risk assessment results and supports effective management decisions, ensuring the prioritization and proper protection of critical resources.

Keywords

fuzzy cognitive maps, information security risk management, SADT

1. Introduction

Information systems used today to store and process large volumes of critical information are increasingly exposed to complex and diverse threats driven by rapidly evolving technologies, such as the Internet of Things (IoT), artificial intelligence (AI), and cloud computing. These advancements enable cybercriminals to employ sophisticated attack methods that are more challenging to detect, thereby presenting significant obstacles to traditional security systems. Such systems are no longer capable of effectively countering these threats without continuous adaptation to new conditions. In light of these challenges, international information security standards, such as ISO/IEC 27001:2022,

CH&CMiGIN'24: Third International Conference on Cyber Hygiene & Conflict Management in Global Information Networks, January 24–27, 2024, Kyiv, Ukraine
* Corresponding author.
† These authors contributed equally.
y.kostiuk@kubg.edu.ua (Y. Kostiuk); p.skladannyi@kubg.edu.ua (P. Skladanny); juliyasamoil@gmail.com (Y. Samoilenko); karynakhorolska@gmail.com (K. Khorolska); b.bebeshko@kubg.edu.ua (B. Bebeshko); v.sokolov@kubg.edu.ua (V. Sokolov)
0000-0001-5423-0985 (Y. Kostiuk); 0000-0002-7775-6039 (P. Skladanny); 0000-0003-3787-1435 (Y. Samoilenko); 0000-0003-3270-4494 (K. Khorolska); 0000-0001-6599-0808 (B. Bebeshko); 0000-0002-9349-7946 (V. Sokolov)

which specifies requirements for information security management systems, and the NIST Cybersecurity Framework (CSF), serve as essential tools for enterprises aiming to develop effective and adaptive security systems [1–5].

In this context, risk management in information security is becoming increasingly important as an integral component of enterprise strategy [6–14]. Effective risk management requires the accurate assessment and classification of information resources, detailed analysis and forecasting of potential threats, and the timely implementation of appropriate countermeasures to reduce the likelihood of successful attacks on the system [15–22]. Additionally, the integration of advanced technologies, such as machine learning and automated monitoring systems, plays a crucial role in enabling early anomaly detection and breach prevention [23–31]. Standards like ISO/IEC 27005:2018 offer clear methods and recommendations for conducting risk assessments, assisting businesses in prioritizing risk management efforts and correctly applying countermeasures [32–38].

It should also be noted that traditional methods of assessing information resources, which rely on a simple ranking of resources using quantitative or qualitative criteria, are no longer sufficient to provide a comprehensive and accurate picture of risks. This limitation is particularly evident given the current level of information technology development and the complexity of interdependencies among components in distributed systems. For instance, interactions between servers in a cloud environment can significantly alter the overall threat landscape, where even a minor vulnerability in one component can lead to severe consequences. This consideration has become the foundation for new standards, such as ISO/IEC 27035, which outlines security incident response processes. These processes incorporate detailed risk assessments, including the evaluation of dependencies between infrastructure components [1, 8, 14, 39–46].

Therefore, this paper proposes an approach to the assessment of information resources that not only considers their importance and criticality to the enterprise's business processes but also enables a detailed analysis of their interdependencies. Such an analysis is crucial for generating accurate and reliable risk assessments, as practice shows that disregarding the relationships between different resources can result in significant errors, particularly in a rapidly evolving technological environment [3–5, 9]. To enhance the accuracy of risk assessments, it is essential to adopt new methodologies, such as those recommended in ISO/IEC 27019. This standard addresses specific aspects of cybersecurity for critical infrastructure, offering a more comprehensive approach to assessing and mitigating risks arising from resource interactions across various levels of the enterprise [6, 16, 25].

2. Literature review

The methodology for ensuring enterprise information security based on information risk assessment using FCMs represents a comprehensive approach. It enables not only the visual evaluation of the potential impact of major threats on an enterprise's information system but also the effective systematization of risk factors within a broader analysis of information security. By integrating traditional risk assessment methods with advanced technologies, this approach provides a more precise analysis of the impact of threats on critical enterprise resources [1–4, 6, 10–13].

Assessing information security risks is an essential component of ensuring the stable operation of an enterprise amidst the growing landscape of threats, particularly those associated with digitalization and globalization. The advancement of modern technologies further underscores the urgency of employing contemporary methods for risk assessment and management. As enterprise information resources often constitute vulnerable elements within IT infrastructures, effective risk management is critical to safeguarding their security [2–5, 7, 12].

Modern approaches to information security risk management incorporate both quantitative and qualitative assessment methods, enabling the evaluation of interdependencies among various enterprise resources and their significance to business processes. Notably, models that integrate external threats provide a more comprehensive understanding of risks. For instance, studies by Sharma and Shahi, among others, demonstrate the use of neural networks to predict threats based on historical data, offering valuable insights for proactive risk management [9–13, 15, 18].

Another example is the work of Bensou and Martinez, who developed a context-based risk assessment methodology. This approach not only evaluates the value of assets and the threats they face but also considers how these assets interact with the external environment, including other businesses and government agencies. By incorporating these interactions, the methodology provides a more accurate determination of the level of exposure enterprises face in the rapidly evolving digital landscape, particularly in scenarios involving attacks on supply chains or critical infrastructure [11, 19–22].

The FCM methodology, as part of this system, enables the assessment of both the likelihood and impact of threats while also identifying critical points within the enterprise's information system. This approach facilitates more precise risk assessments and the implementation of appropriate countermeasures to mitigate potential losses. Such capabilities are especially vital in a world where emerging technologies, including artificial intelligence, the Internet of Things (IoT), and cloud computing, are continuously reshaping the nature and scope of threats.

Given these trends, this paper proposes a methodology for assessing information resources that not only accounts for their significance to an enterprise's business processes but also provides a detailed analysis of their interdependencies—an aspect crucial for achieving accurate risk assessments. Furthermore, innovative risk management approaches based on SADT technology facilitate the identification of key concepts, the recognition of critical resources, and the uncovering of relationships among them. This, in turn, significantly enhances the effectiveness of risk mitigation and information security measures [6–8, 23–24, 31–35].

Another crucial step is the integration of risk management into cybersecurity processes at the strategic level. Following the recommendations of Curtis and Chen, the increasing prevalence of cyber threats necessitates a cybersecurity strategy that embeds risk management as a core component of corporate culture and management practices. This approach aims to proactively prevent data breaches, cyber fraud, and other criminal activities [9, 13–17].

Thus, utilizing fuzzy cognitive maps to assess an enterprise's information risks enables the integration of advanced technologies into the risk management process, ensuring a comprehensive approach to mitigating potential threats.

To identify the key concepts (information resources, threats, and vulnerabilities) necessary for this study, it is proposed to use systematic modeling of information security risk management processes based on the Structured Analysis and Design Technique (SADT). SADT is a methodology for structural analysis and design that is widely used to model complex systems and processes. It has proven effective in the design of risk management systems, as it enables the visual modeling of processes and supports informed decision-making. This approach facilitates the identification of relationships and informational content within these processes, the classification of an enterprise's primary information assets, the identification of the most critical resources, and the determination of the required levels of protection. The primary objective of SADT is to create a clear, logically structured framework that explains how a system operates, how its components interact, and which components are critical to achieving the desired outcomes [5, 8, 12]. In the context of information security risk management, SADT allows for the modeling of processes and the analysis of relationships among information resources, threats, and vulnerabilities. This enhances the ability to identify system vulnerabilities more effectively and plan protective measures accordingly.

Therefore, this paper proposes an approach to the assessment of information resources that not only considers their importance and criticality to the business processes of an enterprise but also includes a detailed analysis of their interdependencies. Such analysis is crucial for generating accurate and well-founded risk assessments. As practice demonstrates, disregarding the interrelationships between different resources can result in significant errors in risk evaluation, particularly in a rapidly evolving technological environment [7–9, 16]. To enhance the accuracy of risk assessments, it is essential to adopt new methodologies, such as those outlined in ISO/IEC 27019. This standard addresses specific aspects of cybersecurity for critical infrastructure and provides a more holistic approach to assessing and mitigating risks associated with resource interactions at various levels within the enterprise [25–29].

3. Methods

The study of dependencies between information resources, as illustrated in the simplified model shown in Figure 1, enables a deeper analysis of the relationships within an enterprise's information infrastructure, while accounting for modern security requirements. These dependencies are organized into a hierarchical structure, with the building serving as the highest-level node. The physical integrity of this node underpins all other enterprise resources. In the event of its destruction, and without the availability of data backups or alternative information processing centers located in other facilities, all critical information assets would effectively be lost [2, 16–19, 26, 39–41]. However, it is important to recognize that, in practice, most modern enterprises implement strategies involving multi-level redundancy and business continuity. These strategies often leverage cloud technologies, virtualization, and automated disaster recovery systems to mitigate the risks associated with such dependencies [3, 11–15].

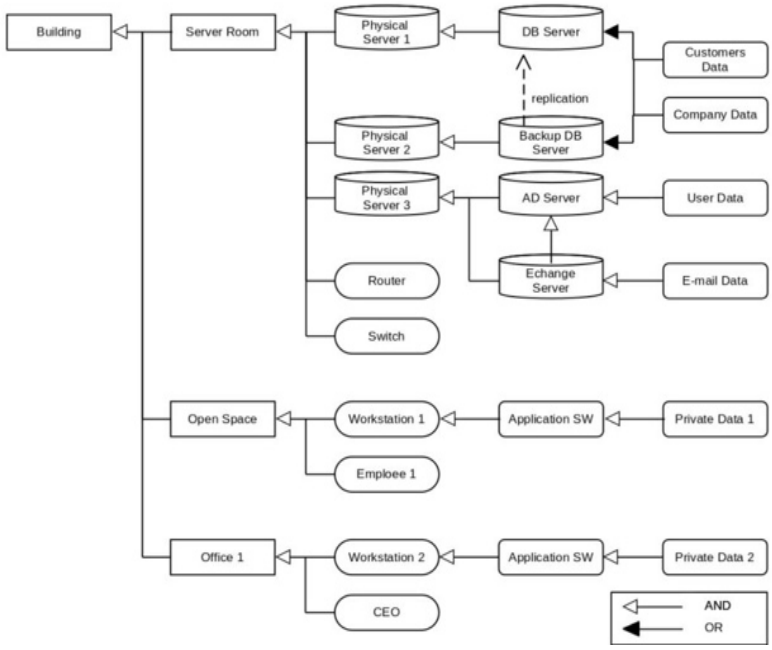

Figure 1: Relationships between enterprise information resources.

As the analysis reveals, a single information resource may depend on multiple others, significantly increasing the complexity of managing such systems. For instance, an Exchange server may depend simultaneously on both physical server 2 and an Active Directory server, creating a complex web of infrastructure interdependencies that must be carefully considered when designing a security strategy. Modern risk management methods, particularly those incorporating the concepts of Business Continuity and Disaster Recovery, emphasize the examination of all potential points of failure. These include not only physical components but also network and software resources, ensuring a comprehensive approach to minimizing risks [6, 39, 41].

When analyzing the database server, it is evident that a redundancy mechanism is in place—the company employs an additional server capable of handling the load in the event of a failure of the primary server. This ensures uninterrupted access to critical data [7]. However, for effective risk management, it is essential to account for the complex interdependencies among the data stored on these servers. Even a minor error in modeling these dependencies can result in significant consequences during an incident [8]. Furthermore, the integration of advanced technologies, such as artificial intelligence, machine learning, and automated monitoring systems, enables not only the prediction of potential failures but also rapid responses to emerging threats. This significantly enhances the security and stability of the enterprise's information infrastructure [9].

When developing a modern model of information risk management for an enterprise, several key assumptions can be made to determine the effectiveness and depth of the analysis of dependencies between information resources and infrastructure elements. The first assumption is that the business goals of the enterprise are directly influenced by all the end elements in the hierarchy of the information resource system [10]. Consequently, ensuring the proper functionality and security of the organization requires guaranteeing the confidentiality, integrity, and availability of data and other critical resources, in alignment with the established hierarchy of dependencies [11, 17]. For instance, user data in such a hierarchy follows a clearly defined chain of dependencies, beginning with the Active Directory server and extending to the physical location of the building. Since enterprise infrastructures are continually exposed to risks from cyber threats, natural disasters, and technical failures, it is important to recognize that most modern companies actively adopt strategies for multi-level redundancy and business continuity. These strategies often involve the use of cloud technologies, virtualization, and automated disaster recovery systems [12]. Such measures not only mitigate the impact of physical disasters on operations but also enable rapid recovery from cyberattacks or failures, ensuring greater resilience and operational stability.

Additionally, for a more precise risk assessment, it is essential to assign a specific weight to each element in the dependency chain. This weighting enables a more efficient analysis of risks based on particular threats. For example, if one element depends on another that carries a high level of risk (e.g., due to software vulnerabilities or unresolved configuration errors), this risk should be proportionally transferred to the dependent element to accurately represent its contribution to the overall security posture of the organization [13, 17, 39–41]. In the case of redundant or duplicated infrastructure elements (e.g., a backup server taking over if the primary server fails), the OR connection type is used. This approach reduces the overall risk level, as the risk is distributed among multiple components that perform the same functions. Conversely, the use of the AND connection type—where a dependent element relies on only one specific higher-level element—provides a clear delineation of the dependency chain, ensuring transparency in business continuity planning [10, 14, 24].

In general, the adoption of modern approaches to risk modeling provides a more accurate representation of dependencies within a system, which is critical for managing enterprise cybersecurity, particularly in the face of contemporary threats such as cyberattacks, phishing, and insider threats [1, 3, 4, 19–23, 30–32, 39, 40]. With the advancement of cutting-edge technologies, such as artificial intelligence (AI) and machine learning (ML), it has become possible to automatically detect and predict risks through big data analysis. This capability enables not only the timely identification of vulnerabilities in information systems but also rapid responses to potential threats, thereby enhancing the overall level of protection. In particular, automated monitoring systems play a crucial role by detecting anomalies in real time, ensuring a more efficient and swift response to emerging threats.

In the context of risk modeling for our information system, risk values can be assessed using a 4×4 risk matrix (Figure 2), which serves as an effective tool for classifying the likelihood of threats and evaluating their impact. In this matrix, the probability of a threat is represented by the columns, while the level of impact is represented by the rows. The following categories are used to classify risks: from 1 to 5—low risk; from 6 to 9—medium risk; from 10 to 16—high risk. This structured approach enables a clear and systematic evaluation of risks, facilitating better decision-making in the management of information system security [33–35].

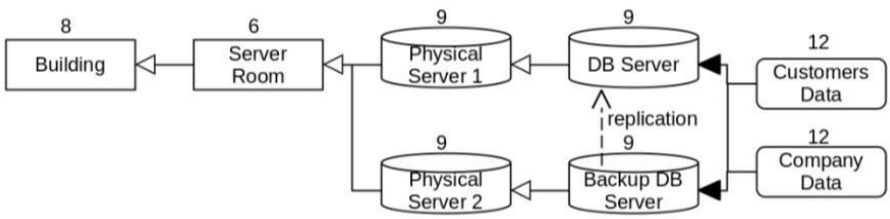

Figure 2: The value of risk.

Although this matrix offers a clear understanding of the probability and potential impact of threats on various elements of the system, it is important to note that, in practice, it is not always possible to determine these values with precision. This challenge is particularly relevant in the context of rapidly evolving technologies and continuously emerging threats. Therefore, in the subsequent stages of the analysis, these intervals will be used to enable a more flexible risk assessment. This approach allows for the consideration of diverse scenarios and potential outcomes, ensuring a more adaptive and comprehensive evaluation of risks.

Thus, the utilization of the 4×4 risk matrix, combined with the consideration of all critical aspects of risk management, enables enterprises to effectively identify key points of vulnerability. This approach facilitates the development of comprehensive protection strategies that encompass both technical and organizational measures. These strategies are designed to mitigate risks and ensure the continuity of business processes, even in the event of serious incidents [17–19].

4. Design of a dependency assessment model for an enterprise information system

When designing a dependency assessment model for an enterprise information system, it is essential to address both the technical and organizational aspects of risk management. Given the prevalence of modern threats and the rapid pace of technological advancements, such models must be flexible and capable of adapting to new conditions. To achieve this, a well-defined algorithm is employed to construct a comprehensive view of risks and dependencies within the system. This approach ensures an effective evaluation of the risk level associated with each element, enabling informed decision-making and improved security measures [25, 36–38].

The risk management process is conducted in several stages. During the preparatory stage, the information system is divided into subsystems and individual elements, followed by an expert assessment of the significance level of each subsystem. At the stage of risk assessment for the system, subsystems, and elements, the composition and number of elements within each subsystem are identified. Additionally, an expert evaluation of the characteristic criteria for each element is performed based on predefined categories, and the risks are calculated for each subsystem and for the entire system as a whole [20–24]. The subsequent step involves determining the adequacy of the risk level. A risk is deemed adequate if its level is classified as “below average” or “low”. If the risk level is found to be inadequate, plans and measures are developed to mitigate these risks. Alternatively, in cases of repeated application of the methodology, adjustments are made, with these refinements being implemented in practice.

The risk of an individual element of a subsystem of a certain type is determined by the formula:

$$R = ICVP, \tag{1}$$

where I—is the degree of interest of the attacker in attacking elements of this type, C—is the degree of damage to the subsystem from the consequences of a possible attack on elements of this type, V—the degree of vulnerability of the horns of this type, P—the degree of probability of an attack on an element of this type. The specific risk of homogeneous elements is calculated as follows:

$$R = \frac{N_j}{N} R_j, \tag{2}$$

where Rj—is the risk of an individual element of the subsystem j-of the subsystem, Nj—is the number of homogeneous elements j-of the -th type in the subsystem, N—is the total number of elements of all types in the subsystem. Subsystem risk:

$$R = S \sum_{i=0}^{k} (R), \tag{3}$$

where S—is the degree of importance of the subsystem, R—is the specific risk of homogeneous elements, k—number of types of elements.

The total risk of a subsystem can be calculated as the sum of the risks of all its elements:

$$R = \sum_{i=0}^{n} R_{C_i}, \quad (4)$$

where Ri—risk i-of the subsystem, n—is the number of subsystems in the system.

Analyzing formulas (1), (2) and (4), we can conclude that, with equal risk parameters of individual elements of each subsystem, the risk of the entire system is a power function of the form $f = kx4$. The formula for calculating the risk is as follows:

$$R_i = k \cdot B_i^4, \quad (5)$$

where Ri—is the risk of the whole system in i-is the state of equality of risk levels of its elements in conventional units, k—is the system constant when operating in this configuration, Bi—is the risk level of the system in terms of expert assessments in i-the state of equality of risk levels of its elements.

Obviously, the parameter Bi reflects a qualitative assessment of the system's risk. From formula (5) we can express:

$$k = \frac{R_i}{B_i^4}, \quad (6)$$

$$B_i = \sqrt[4]{\frac{R_i}{k}}, \quad (7)$$

The resulting value Bi can be translated into a qualitative assessment using the scale used: to do this, round it to the nearest whole number and determine which level of risk it corresponds to on the scale. The degree of assessment is ranked on a five-point scale, where 1 is low and 5 is high. The risk is calculated for each resource of the structure: "subsystem element—subsystem—system". Expert assessments are used to rank the risks of indicators for each element of the subsystem. The risk for the entire system is defined as the arithmetic mean of the risks of subsystems.

The following indicators are used for risk assessment: S—level of subsystem significance (indicator of "destructiveness") —conditional ranking of subsystems in the hierarchy of the entire system, determined by the degree (contribution) of a particular subsystem to the functioning of the entire system; N—number of elements of this type—the number of elements in the subsystem that ensure the performance of technological functions; I—the degree of interest of the attacker in attacking the element—the measure of interest on the part of the attacker in performing unauthorized actions; C—the degree of damage from the consequences of an attack on an element—the degree of damage caused in the event of a successful threat; V—the degree of vulnerability of the element—the degree of change in the technological properties of the element in the event of a successful threat; P—the degree of probability of an attack is a measure of the probability of successful unauthorized actions by an attacker that lead to changes in the functional characteristics of the system or obtaining confidential information.

Expert opinions were obtained through the use of questionnaires. These questionnaires consist of scoring sheets that include a list of resources, indicators, and criteria used to evaluate the degree of risk.

The risk assessment utilized the following criteria for each indicator: the attacker's interest in targeting the element, the damage resulting from the attack, the vulnerability of the element, and the likelihood of the attack being realized. An attacker's interest may stem from access to commercial or technical information, personal gain, or unmotivated malicious intent. Damage is assessed based on the element's interconnections with other parts of the subsystem, the consequences of its failure, and the costs associated with mitigating the impact of an attack. Vulnerability considers the physical accessibility of the element as well as its susceptibility to informational and mechanical vulnerabilities. Likelihood of an attack is determined by the effectiveness of existing protection mechanisms, the element's ability to resist attacks and physical impact, and the historical analysis of similar attacks on analogous elements. Once experts evaluate each criterion, the arithmetic mean for each element is calculated, and the resulting score is rounded to the nearest whole number. Risks are

assessed on a five-point scale, ranging from minimum to maximum risk. The methodology employs a dynamic algorithm that accounts for the interconnections among elements and subsystems at all levels of operation. Since monitoring systems are integral to enterprise infrastructure, this methodology can be adapted for assessing the risks of other enterprise information systems. This adaptability is particularly effective due to the interdependence of assets, which can be analyzed using cognitive maps.

The first step in constructing a dependency assessment model for an enterprise information system is to identify the highest level in the hierarchy of the enterprise's information resources. This typically includes critical elements such as the main server or a key building that serves as the operational hub. Starting with the most critical components enables the assessment of dependencies on these elements and provides a foundation for progressively analyzing smaller, yet equally significant components. This hierarchical approach ensures the integrity of the analysis and facilitates an accurate evaluation of the impact each element has on the overall security of the enterprise [26–29, 31].

The next step is to assign weights to the three main components of dependencies: privacy $Wcon$, $Wint$ and $Wava$. These components are key to determining the level of importance of each element in the context of security and its vulnerability to various threats. The weight of each component is estimated on a scale from 0 to 1 in increments of 0.1, which allows you to accurately reflect the importance of each aspect for a particular element [30–35]. This approach provides a more detailed assessment of dependencies in the system and allows you to identify even non-obvious vulnerabilities that may affect security.

After determining the weights of the components, the next step is to adjust the risks using a specialized dependency formula [34–38]. This formula enables the consideration of not only individual elements but also their interrelationships. For instance, in cases where elements are connected according to the OR principle, the risk for each component is adjusted using the average value of the adjusted risks of the interconnected elements. Conversely, for elements that depend on multiple other components, the adjustment must account for all higher levels of dependencies. This means that if one element relies on several others, accurately determining its risk level requires incorporating the risks of all these elements as well as their interactions.

Further risk adjustments are made using special formulas:

$$W_0 = \sum_{i=con.int.ava} W_i, \tag{8}$$

$$W_0 \times max\ (W_{con}, W_{int}, W_{ava}) \times RV, \tag{9}$$

where $W0$—is the total dependency weight for the element, $Wcon$, $Wint$ and $Wava$—are the weights of the dependency components, and RV (Risk Value) is the risk value for the higher-level entity to which the current entity is related. The formula allows you to adjust the risk value depending on the weight of the components and the type of connection of the elements.

In the real world, accurate risk assessment can be challenging due to rapidly changing technologies and the continuous evolution of threats. Therefore, the application of such models necessitates constant updating and adaptation. To address this, intervals of risk values are employed to create a more flexible model for risk assessment and forecasting [17, 29]. Incorporating these intervals allows for the identification of potential threats, even in scenarios that were not initially considered during the early stages of the analysis.

The total weight of dependencies, determined by the sum of the component weights and their maximum value, enables the construction of a comprehensive picture of dependencies for each element within the system. Notably, the risk adjustment process can incorporate advanced technologies, such as cloud services and automated monitoring systems, which facilitate the real-time identification of potential threats [6–8, 19–22]. These innovations not only enhance the effectiveness of risk assessment but also enable faster and more efficient responses to potential security incidents.

An example of risk adjustment:

1. Low dependence and low risk: If an asset has a low dependence on a low-risk element (RV = 1), the risk adjustment can be as little as +1 point.
2. Medium dependence and medium risk: in the case of medium dependence and medium risk (RV = 2), the risk adjustment can be increased by +2.4 points.
3. High dependence and high risk: If an asset is highly dependent and exposed to a high risk element (RV = 3), the risk adjustment can be significant—by +7.2 points.

These adjustments allow for a more accurate reflection of the real level of risk and enable an enterprise to develop more effective strategies for protecting its information resources [9–12].

As a result of applying this dependency assessment model, an enterprise receives a clear picture of potential threats, which allows it to respond quickly to possible incidents and increase the overall level of cybersecurity in a rapidly changing threat environment.

Figure 3 shows part of the enterprise model, where each infrastructure element is assigned the appropriate weights for the dependency components.

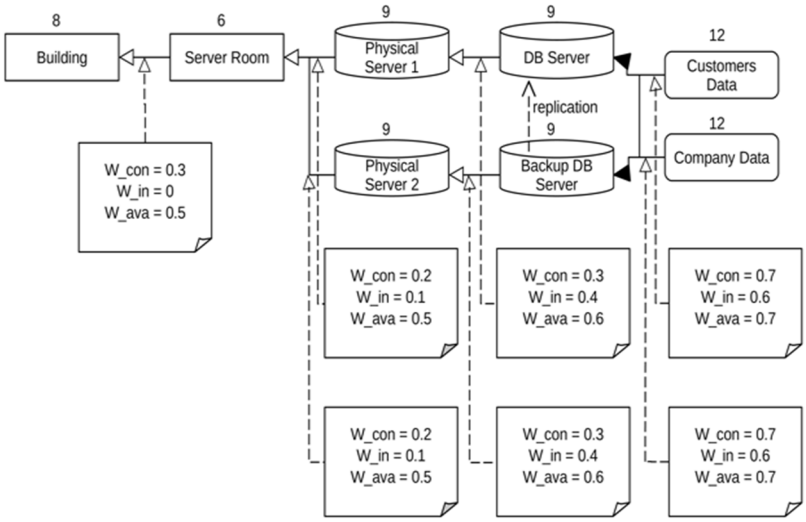

Figure 3: Determining dependency weights for infrastructure elements.

Each element is assessed in the context of the risks associated with its dependencies on other elements [13]. It is important to note that, following the initial risk assessment for each organizational element, these values are adjusted based on the actual dependencies between the elements [14–16]. For instance, when assessing customer data, we consider not only its direct vulnerability but also the elevated risk level of the database servers that store this data. This approach provides a more accurate representation of the actual threat level to the information.

It should also be noted that the adjustment of risk values depends on the availability of redundant infrastructure elements. For example, for customer data with duplication at the database server level, the risk adjustment is limited to +2.1, as the presence of redundant resources mitigates the potential impact of the threat [18]. However, certain key system elements, such as private data, require significant adjustments to their risk values. This is because such data has dual dependencies—on both the Active Directory server and the physical server. These additional dependencies introduce heightened vulnerability, necessitating an increase in the risk level by +4 points [19–21].

Algorithms for assessing the security of enterprise information resources can be based on the use of FCM. A cognitive map is a sign-oriented graph where the key factors of the modeling object (concepts) are interconnected by arcs that reflect cause-and-effect relationships. These connections characterize the degree of influence of concepts on each other and are set using fuzzy WijWij weights in the form of interval scores or linguistic terms. In general, a fuzzy cognitive map is defined as a tuple of sets [20–22]:

$$FCM = \{C, F, W\}, \tag{10}$$

where FCM—is an oriented graph specified by a tuple of sets: $C = \{Ci\}$—a finite set of vertices (concepts), $F = \{FK\}$—is a finite set of links between concepts (the set of oriented graph arcs), and $W = \{Wij\}$—a finite set of weights of these connections. Figure 4 shows an example of building an FCM for assessing information risks of an enterprise. In the example of building an FCM for assessing information risks of an enterprise, the concepts are divided into five types: CG—a set of target factors, CU—a set of destabilizing factors (threats), CS—set of information resources, CI—set of basic factors (intermediate concepts indicators), CR—a set of controlling factors [4, 9]. The weights of the links were determined on the basis of expert assessments using linguistic variables ("weak", "medium", "strong") on a scale of [0,1]. Three main factors were selected as the target concepts to be analyzed: "Reputation", "Quality of products/services" and "Material and technical condition", which reflect the general state of the enterprise in the market [4–7].

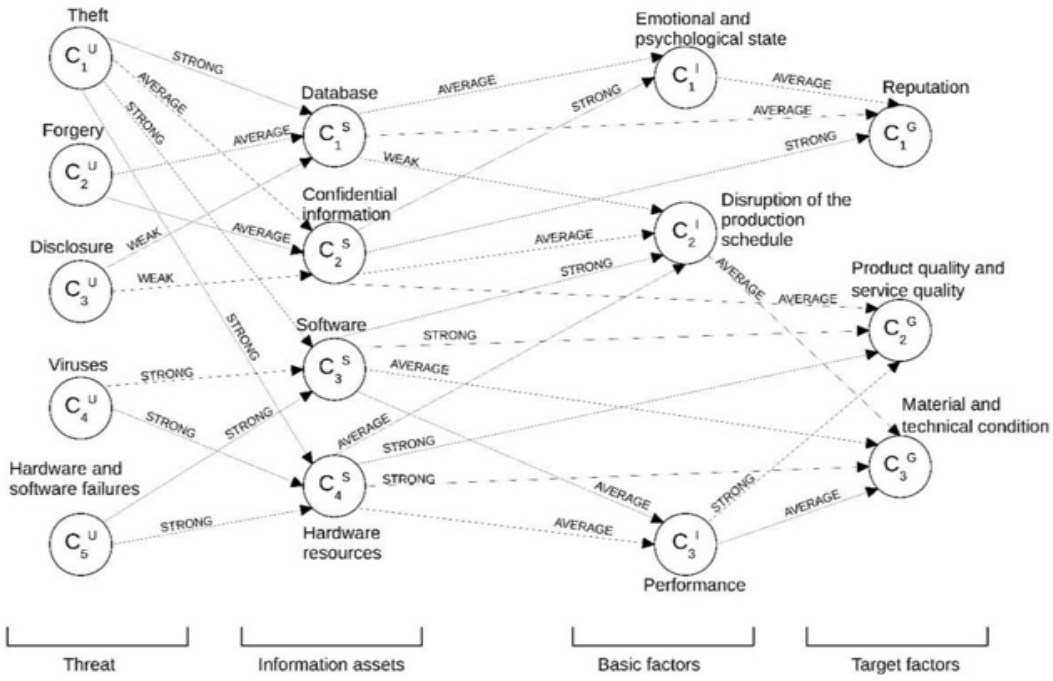

Figure 4: FCM for assessing information risks of an enterprise.

The FCM built in this way allows us to assess the impact of both individual threats and their combination on a particular target factor. The overall effect of the impact of the concept CUi (threat) on the concept CjG (target factor) is determined using the reach matrix:

$$T = \sum_{i=1}^{n-1} Wi, \tag{11}$$

$$Wi = \|Wij\| n \times n, \tag{12}$$

where$Wi = \|Wij\| n \times n$—is the adjacency matrix of the FCM, Wij—is the weight of the link between i-m and j-FCM concepts, n—is the number of FCM concepts [8, 9]. With fuzzy values of weights Wij the multiplication and addition operations are replaced by the operations of finding the minimum and maximum, respectively. The indirect effect of the impact CUi on CjG is determined by the minimum value of the weights of the links in the path:

$$Tk(CUi \rightarrow CjG) = min\{Wij\}. \tag{13}$$

The full (total) effect of the impact on $C^{U}{}_{i}$ on $C_{j}{}^{G}$is determined by adding up all the values of the links that exist between the concepts

$$I(CUi \rightarrow CjG) = max\{I1, T2, \ldots TN\}, \tag{14}$$

where Tk—is the indirect effect between the threat CUi and the target factor CjG{Wij}—is the set of weights of links on the path between concepts CUi and CjGN—is the number of indirect effects (i.e., the number of paths between concepts CUi and CjG) [10–12].

Table 1 presents the concepts selected for analysis and their variable states, offering a generalized example of how concepts can be defined within the framework of FCMs for assessing enterprise information risks. It is crucial to note that transitions between the different states of each concept are guided by expert opinions or the results of risk analysis [13].

Risk j-of the target factor in relation to the i-threat is determined by the formula:

$$Rij = PI\ T(CUi \rightarrow CjG)\ rj, \tag{15}$$

where rj—value j-of the resource, $T(CUi \rightarrow CjG)$—is the full effect of the threat CUi on CjG, PI—is the probability of realization i-of the threat being realized.

The total risk R for the considered set of threats is defined as:

$$R = \sum_{i=1}^{m} \sum_{j=1}^{k} V_J R_{IJ}, \tag{16}$$

where m—is the number of threats, k—is the number of target factors, and V_J—is the significance of the j-of the target factor determined by experts [14, 15].

Table 1
Concepts and Their Variable States for Analyzing Enterprise Information Risks

Con-chain	Concept name	Type of concept	Variables states
C_1U	Theft	Destabilizing factor (threat)	$\mathbf{x}_1$: the average number of thefts per unit of time.
CU_2	Modification	Destabilizing factor (threat)	$\mathbf{x}_2$: the average number of unauthorized modifications per unit of time.
CU_3	Disclosure	Destabilizing factor (threat)	$\mathbf{x}_3$: the average number of disclosures per unit of time.
CU_4	Viruses	Destabilizing factor (threat)	$\mathbf{x}_4$: the average number of virus attacks per unit of time.
CU_5	Hardware and software failures	Controlling factor	$\mathbf{x}_5$: the average number of hardware and software failures per unit of time.
C_1S	Databases	Basic factor	$\mathbf{x}_6$: the level of reliability of information in databases, %.
C_2S	Confidential information	Target factor	$\mathbf{x}_7$: level of confidentiality, %.
C_3S	Software.	Target factor	$\mathbf{x}_8$: software availability level, %.
C_4S	Hardware resources	Basic factor	$\mathbf{x}_9$: operability of computers and other equipment, %.
$C1I$	Emotional and psychological state	Destabilizing factor (threat)	$\mathbf{x}_{10}$: number of stressful situations or incidents, units.
$CI2$	Violation of the company's work schedule	Destabilizing factor (threat)	$\mathbf{x}_{11}$: the number of production schedule disruptions, units.
$CI3$	Qualification level of employees	Target factor	$\mathbf{x}_{12}$: the average level of qualification of employees on a five-point scale.
C_1G	Reputation of the company	Target factor	$\mathbf{x}_{13}$: number of negative publications or statements, units.
CG_2	Quality of service provision	Target factor	$\mathbf{x}_{14}$: the share of employees who successfully work in their specialty, %.
CG_3	Material and technical condition	Basic factor / Controlling factor	$\mathbf{x}_{15}$: capitalization, UAH.

Table 2 presents estimates of the impact of threats $C_1{}^U$–$C^U{}_5$ on the target factors $C_1{}^G$–$C^G{}_3$. The analysis of the FCM shows that, given the strength of the connection between the concepts, the realization of the threat "Theft" in relation to the information resources of the enterprise "strongly" affects the concepts "Quality of products/services" and "Material and technical condition" and "moderately" affects the concept "Reputation" of the enterprise [19–22, 40–43]. By determining the value of the target factors in absolute or conditional units $C^U{}_i$ it is possible to calculate the potential risk (damage) both for individual target factors from the impact of certain threats and the overall (total) risk [18, 39–41].

The use of the FCM makes it possible not only to visually identify the negative processes that occur in the information system under the influence of threats, but also to identify the most vulnerable areas and ways to reduce the impact of threats through the introduction of appropriate

control measures (countermeasures) {CRk} which allows to reduce the level of information risks to an acceptable value. For example, if viruses are considered as a threat to the company's information resources (concept C$U4$), and the level of impact of this threat on the target factors C$G2$ ("Quality of products/services") and C$G3$ ("Material and technical condition") is defined as "strong", then to reduce this impact, it is necessary to implement such countermeasures as choosing an anti-virus protection strategy, selecting an appropriate anti-virus program, managing anti-virus tools, etc. This will reduce the degree of influence of the concept C$U4$ on the concepts C$G2$ and C$G3$ to the "medium" level [16, 17, 39, 41–43]. Table 3 shows the recommended measures (a set of controlling factors) and estimates of the degree of their impact on the mentioned concepts. The corresponding FCM after the introduction of countermeasures (concepts C1R–CR31) is shown in Figure 5.

Table 2
Assessment of the Degree of Impact of Threats on Target Factors

The threat (C^U_i)	The full effect of the threat on the target factor before countermeasures are taken			The full effect of the threat on the target factor after the introduction of countermeasures		
	C$\boldsymbol{G_1}$	C$\boldsymbol{G_2}$	C$\boldsymbol{G_3}$	C$\boldsymbol{G_1}$	C$\boldsymbol{G_2}$	C$\boldsymbol{G_3}$
C_1U	average	strong	strong	weak	average	average
CU_2	average	average	average	weak	weak	weak
CU_3	weak	weak	weak	weak	weak	weak
CU_4	-	strong	strong	-	average	average
CU_5	-	strong	strong	-	average	average

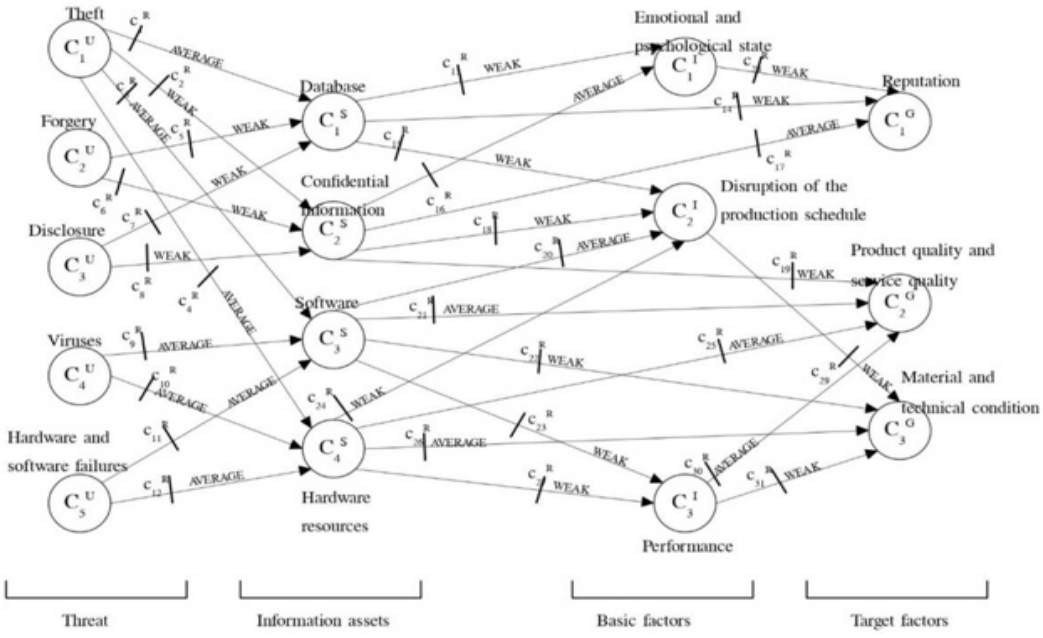

Figure 5: FCM for assessing information risks of an enterprise taking into account a set of controlling factors.

An analysis of the ratio between risks and the costs of mitigation measures enables the identification of rational approaches to managing an enterprise's information security and justifies the necessary expenditures on security. Decision-making regarding the selection of appropriate countermeasures and the evaluation of acceptable risk levels should be guided by the cost-effectiveness criterion [2, 16, 40–43]. In this context, the following formulations of tasks for selecting control factors to reduce risks are possible:

1. $R_\Sigma \le R_{add}$ when $S_\Sigma \to min$ —determining the minimum costs of implementing information security measures while ensuring an acceptable level of risk;
2. $S_\Sigma \le S_{add}$ when $R_\Sigma \to min$—minimizing risk at a given cost of implementing measures [9].

Here R_Σ and S_Σ—total risk and costs of information security measures (countermeasures), R_{add} and S_{add}—permissible values of the total risk and costs.

The effectiveness of controlling influences is calculated by the formula:

$$\eta = \frac{R_\Sigma^{/} - R_\Sigma}{R_\Sigma^{/}} \times 100\%, \quad (17)$$

where $R_\Sigma^{/}$—is the calculated initial risk, and R_Σ—is the risk after the introduction of additional countermeasures.

Table 3
Set of Controlling Factors

Designation	Concept name	The impact of the concept on communication	Designation	Concept name	The impact of the concept on communication
C_1^R, C_5^R, C_7^R	Differentiation of user access levels	average	C_{18}^R	Organization of the document storage procedure	average
$C_2^R, C_6^R, C_8^R, C_3^R C_4^R$	Control and management of access to the premises	average	C_{20}^R	Developing a procedure for recovery from virus attacks	average
C_9^R, C_{10}^R	Development and implementation of the virus protection concept	strong	$C_{19}^R, C_{21}^R, C_{25}^R$	Developing a procedure for prompt response to incidents	average
C_{11}^R, C_{12}^R	Administrative and technical means of controlling the work of users	average	C_{22}^R, C_{23}^R	Use of licensed software, access control	average
C_{12}^R, C_{16}^R	Measures to prevent failures	average	$C_{24}^R, C_{26}^R, C_{27}^R$	Technical support of hardware resources	average
$C_{14}^R, C_{17}^R, C_{28}^R$	Formation of a corporate culture of information security	average	$C_{29}^R, C_{30}^R, C_{31}^R$	Development of measures to improve the stability of production processes	average
C_{15}^R	Backup and restore	strong			

The methodology for ensuring enterprise information security through information risk assessment using FCMs is a comprehensive approach. It enables not only the visual evaluation of the potential impact of major threats on the enterprise information system but also the effective systematization of risk factors as part of a holistic analysis of information security [3, 14, 35–38, 41–43]. This methodology serves as a practical tool to support decision-making across all levels of the enterprise security policy. It enhances the convenience and accuracy of information security management at both strategic and operational levels, enabling the implementation of adaptive and timely management measures.

Automating the processes of analyzing information risks, prioritizing them, and selecting effective countermeasures to protect an enterprise's information assets significantly reduces the time required for comprehensive risk analysis. It also improves the quality of decision-making and helps reduce the costs associated with implementing security measures. This is achieved by structuring all stages of analysis and countermeasure selection. Automation enables the flexible adaptation of security strategies to the enterprise's current needs and facilitates a rapid response to evolving threat conditions.

The proposed structure of the decision support system (DSS) for managing enterprise information risks, based on cognitive modeling, offers enhanced objectivity and efficiency in information security decision-making. Cognitive modeling enables a deeper analysis of the cause-and-effect relationships between threats and risks, facilitates the timely identification of the most vulnerable elements within the information system, and supports the development of adaptive countermeasures [7, 10, 33]. Such a system significantly reduces potential losses from both external and internal threats while ensuring optimal resource allocation and maintaining stable information security.

This approach enables the consideration of interdependencies among various information resources in the process of managing information security risks. It facilitates the analysis of how specific factors can influence the overall security of information assets and the achievement of the organization's information security objectives. In light of current trends in cybersecurity and technologies such as cloud computing, automated recovery systems, and virtualization, it is crucial to account for these dependencies when developing a sustainable risk management model. These technologies not only mitigate the impact of physical disasters on operations but also ensure rapid recovery from cyberattacks, thereby enhancing the resilience of the infrastructure against unpredictable threats [8, 18].

5. Conclusions

The study proposes a method for assessing the dependencies among information resources within an information system, which can significantly enhance the accuracy and efficiency of risk analysis at an enterprise. While similar approaches have been applied in both scientific and practical contexts, the importance of considering these dependencies and their impact on the overall level of risk is becoming increasingly evident and critical amidst modern challenges and rapid technological advancements.

International standards in the field of information security, particularly ISO/IEC 27005:2018, along with established risk management guidelines, emphasize the necessity of incorporating dependencies among information resources into the processes of risk analysis and assessment. This standard highlights the importance of determining the degree of dependency between information resources and their impact on enterprise security, specifically in maintaining the confidentiality, integrity, and availability of data. In this context, the proposed method considers dependencies not only in terms of the direct significance of information resources but also through their role in achieving the strategic goals of the enterprise and their susceptibility to various threats.

Additionally, the dependency assessment model incorporates not only direct connections between infrastructure elements but also considers scenarios where information resources exhibit multiple dependencies or duplication. This approach enables risk mitigation through the redundant allocation of resources or the integration of additional security layers. Such measures are particularly relevant in the context of the increasing adoption of cloud technologies, virtualization, and automated recovery systems.

The method of assessing information risks in an enterprise using fuzzy cognitive maps enables a 1.5 to 2-fold reduction in the time required for decision-making regarding the selection of necessary countermeasures. This approach significantly reduces information risks by implementing effective management actions (countermeasures) while keeping the total cost of information protection within acceptable limits.

Due to its flexibility, the proposed method can be seamlessly integrated into existing risk management processes, enabling the adjustment of risk assessments to account for the real dependencies between information resources. In the future, an extended model can be developed that incorporates quantitative methods to more precisely measure the security status of an enterprise. This advancement will provide timely, accurate, and well-founded data for decision-making, aligning with the requirements of modern cybersecurity and the dynamically evolving threat landscape.

References

[1] P. Curtis, M. Chen, Risk Management in Information Security, Elsevier, 2020.

[2] R. Sharma, R., M. Shahi, Neural Network Models for Cyber Risk Assessment, Springer, 2019.

[3] A. Bensou, R. Martinez, Context-Based Risk Assessment in Cybersecurity, IEEE Transactions on Cybersecurity 12(3) (2020) 45–52.

[4] P. Wang, H. Chen, Fuzzy Cognitive Maps in Information Risk Management, International Journal of Intelligent Systems 36(4) (2021) 1234–1252.
[5] A. Korchenko, A. Golubev, Information Security Risk Assessment: Approaches and Best Practices, Springer, 2018.
[6] X. Zhang, Y. Liu, Advanced Risk Management Models for Information Security Systems, Computer Science and Technology 14(1) (2022) 23–29.
[7] Z. Li, J. Yang, A Comparative Study of Risk Management Frameworks in Cybersecurity, Journal of Cybersecurity Research 8(2) (2021) 157–168.
[8] M. Chen, H. Zhang, Integrating Fuzzy Logic in Information Security Risk Assessment, Journal of Risk Analysis 31(4) (2020) 202–211.
[9] J. Xu, J., X. Wang, Evaluating Cybersecurity Risks: A Fuzzy Approach, International Journal of Information Security 22(3) (2021) 200–210.
[10] Yu. Kostiuk, et al., Information and Intelligent Forecasting Systems Based on the Methods of Neural Network Theory, Smart Information Systems and Technologies (SIST) (2023) 168–173
[11] K. Tan, H. Zhou, Assessment of Information Security Risks Using Machine Learning Algorithms, Journal of Network and Computer Applications 54(6) (2021) 81–89.
[12] R. Gupta, P. Singh, Cyber Risk Quantification and Mitigation Using Advanced Analytics, Springer, 2020.
[13] Yu. Kostiuk, et al., Information Protection and Data Exchange Security in Wireless Mobile Networks with Authentication and Key Exchange Protocols, Electronic Professional Scientific Journal "Cybersecurity: Education, Science, Technology" 1(25) (2024) 229–252. doi: 10.28925/26634023.2024.25.229252.
[14] V. Ravichandran, Cybersecurity Risk Management and Mitigation Strategies, Elsevier, 2021.
[15] O. Kryvoruchko, Y. Kostiuk, A. Desiatko, Systematization of signs of unauthorized access to corporate information based on application of cryptographic protection methods, Ukrainian Scientific Journal of Information Security 30(1) (2024) 140–149.
[16] W. Shen, L. Zhang, A Review of Cyber Risk Management Strategies for Enterprises, Journal of Information Security and Applications 23(1) (2021) 72–85.
[17] Q. Liu, Y. Wang, Fuzzy Risk Analysis in Information Security Systems, International Journal of Information Technology 10(5) (2022) 233–241.
[18] Yu. Kostiuk, et al., Integrated protection strategies and adaptive resource distribution for secure video streaming over a Bluetooth network, Information technology 4(6) (2024) 14–33.
[19] T. Xu, Z. Chen, Advanced Risk Management Methods in Cybersecurity and Information Protection, IEEE Access 8(1) (2020) 105234–105242.
[20] X. Zhao, J. Sun, Cybersecurity Risk Management for Cloud Computing Systems, Journal of Cloud Computing: Advances, Systems and Applications 8(4) (2021) 16–28.
[21] Y. Smitiukh, et al., Development of a prototype of an intelligent system for predicting the quality of dairy production, IEEE Intelligent Systems (2022).
[22] O. Kryvoruchko, et al., Analysis of technical indicators of efficiency and quality of intelligent systems, Journal of Theoretical and Applied Information Technology 101(24) (2023) 8127–8139.
[23] S. Wang, T. Zhang, Smart Systems and Cybersecurity Risk Management, Smart Computing Review 12(2) (2021) 46–53.
[24] Yu. Kostiuk, A. Golynskyi, Strategies for integrated protection of wireless sensor networks, Science and Technology Today (Series 'Pedagogy', Series 'Law', Series 'Economics', Series 'Physical and Mathematical Sciences', Series 'Technology') 5(33) (2024) 1232–1247.
[25] Y. Sun, J. Liu, Comprehensive Risk Assessment for Information Security: A Case Study Approach, Journal of Information Technology 35(1) (2022).79–91.
[26] S. Lee, J. Yang, AI-Driven Risk Management in Information Security, Journal of Cyber Intelligence and Data Mining 7(3) (2021) 85–92.
[27] O. Kryvoruchko, Yu. Kostiuk, Development of a Decision Support Information System Based on SYSML, Information Technologies and Society (2(4)) (2022) 58–64. doi: 10.32689/maup.it.2022.2.8.

[28] P. Gupta, A. Soni, Evaluation of Risk Factors in Information Security Using Fuzzy Logic, International Journal of Computer Science and Information Security 18(4) (2020) 191–198.
[29] P. Wang, H. Chen, Fuzzy Cognitive Maps in Information Risk Management, International Journal of Intelligent Systems 36(4) (2021) 1234–1252. doi: 10.1002/int.22345.
[30] R. Sharma, M. Shahi, Neural Network Models for Cyber Risk Assessment, Springer, 1(2) (2019) 34–45. doi: 10.1007/s00542-019-05052-w.
[31] J. Xu, X. Wang, Evaluating Cybersecurity Risks: A Fuzzy Approach, International Journal of Information Security 22(3) (2021) 200–210. doi: 10.1007/s10207-021-005663.
[32] M. Chen, H. Zhang, Integrating Fuzzy Logic in Information Security Risk Assessment, Journal of Risk Analysis 31(4) (2020) 202–211. doi: 10.1111/j.1539-6924.2020.01430.x 33.
[33] A. Bensou, R. Martinez, Context-Based Risk Assessment in Cybersecurity, IEEE Transactions on Cybersecurity 12(3) (2020) 45–52. doi: 10.1109/TCS.2020.2963054.
[34] X. Zhao, J. Sun, Cybersecurity Risk Management for Cloud Computing Systems, Journal of Cloud Computing: Advances, Systems and Applications 8(4) (2021) 16–28. doi: 10.1186/s13677-021-00255-5.
[35] K. Tan, H. Zhou, Assessment of Information Security Risks Using Machine Learning Algorithms, Journal of Network and Computer Applications 54(6) (2021) 81–89. doi: 10.1016/j.jnca.2021.102382.
[36] Q. Liu, Y. Wang, Fuzzy Risk Analysis in Information Security Systems, International Journal of Information Technology 10(5) (2022) 233–241. doi: 10.1007/s41870-02100658-w.
[37] Y. Sun, J. Liu, Comprehensive Risk Assessment for Information Security: Case Study Approach, Journal of Information Technology 35(1) (2022) 79–91. doi: 10.1057/s41265021-00170-7.
[38] R. Gupta, P. Singh, Cyber Risk Quantification and Mitigation Using Advanced Analytics, Springer, 9(2) (2020) 117–126. doi: 10.1007/s10462-020-09744-0.
[39] D. Berestov, et al., Analysis of Features and prospects of Application of Dynamic Iterative Assessment of Information Security Risks, in: Proceedings of Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 2923 (2021) 329–335.
[40] S. Shevchenko, et al., Information Security Risk Management using Cognitive Modeling, in: Proceedings of Workshop on Cybersecurity Providing in Information and Telecommunication Systems II, vol. 3550 (2023) 297–305.
[41] S. Shevchenko, et al., Protection of Information in Telecommunication Medical Systems based on a Risk-Oriented Approach, in: Proceedings of Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3421 (2023) 158–167.
[42] D. Berestov, et al., Synthesis of the System of Iterative Dynamic Risk Assessment of Information Security, in: Proceedings of Workshop on Cybersecurity Providing in Information and Telecommunication Systems II, vol. 3188 (2021) 135–148.
[43] S. Zybin, et al., Approach of the Attack Analysis to Reduce Omissions in the Risk Management, in: Proceedings of Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 2923 (2021) 318–328.
[44] M. Zaliskyi, et al., Heteroskedasticity analysis during operational data processing of radio electronic systems, in: S. Shukla, A. Unal, J. Varghese Kureethara, D.K. Mishra, D.S. Han (Eds.), Data science and security, volume 290 of Lecture Notes in Networks and Systems, Springer, Singapore, 2021, pp. 168–175. doi: 10.1007/978-981-16-4486-3_18.
[45] I. Ostroumov, et al., A probability estimation of aircraft departures and arrivals delays, In: O. Gervasi, et al. (Eds.), Computational Science and Its Applications – ICCSA 2021. ICCSA 2021, volume 12950 of Lecture Notes in Computer Science, Springer, Cham, 2021, pp. 363–377. doi: 10.1007/978-3-030-86960-1_26.
[46] O. Solomentsev, et al., Data processing through the lifecycle of aviation radio equipment, in: Proceedings of IEEE 17th International Conference on Computer Sciences and Information Technologies (CSIT), IEEE, Lviv, Ukraine, 2022, pp. 146–151. doi: 10.1109/CSIT56902.2022.10000844.