INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2026, VOL. 72, NO. 1, PP. 1-10
Manuscript received February 10, 2025; revised January, 2026. doi: 10.24425/ijet.2026.157876

Methods for assessing the effectiveness of information security systems in distributed information systems

Yuliia Kostiuk, Bohdan Bebeshko, Nataliia Kotenko, Natalia Mazur, Karyna Khorolska, and Tetiana Zhyrova

***Abstract*—The article considers methods and approaches to assessing the effectiveness of information security systems in distributed information systems, in particular, a mathematical model for determining the current effectiveness of such systems is derived. The model is based on the calculation of protection potentials, the level of equipment of system elements with security features, and the efficiency of management processes. The article decomposes the main types of threats - theft, copying, disclosure, blocking, modification and destruction of information. To determine the probability of attacks, Bayesian inference and hierarchical analysis (MHA) methods are used to obtain quantitative risk indicators for each category of threat. A new approach to assessing the level of losses arising from the amount of resources required to localize the consequences of attacks is developed. A methodology for modelling the impact of threats using a matrix of pairwise comparisons is proposed, which allows optimising the cost of security measures without increasing the overall cost by replacing expensive methods with alternative more efficient approaches. Particular attention is paid to insider threats, which both attack models and analysis of real incidents confirm. The practical application of the proposed models allows one to increase the efficiency of protection, reduce the cost of system maintenance and ensure its flexibility in responding to constantly changing cyber threats.**

***Keywords*—information systems; security effectiveness; information protection; cyber threats; mathematical modelling; threat decomposition; hierarchical analysis; pairwise comparison matrix; adaptive tuning**

I. Introduction

DISTRIBUTED information systems that support business processes are increasingly vulnerable to sophisticated threats due to the transition from centralised to distributed architectures, which requires an assessment of the security of all elements to maintain the confidentiality, integrity and availability of data [1]. It is essential to analyse the effectiveness of security measures for key information infrastructure systems (KIIS) and critical information systems (CIS), whose stable functioning ensures vital sectors such as energy, transport, finance and healthcare [2]. Disruption of these systems can have catastrophic consequences at the local and global levels.

Incorrect security settings can lead to security breaches or restrictions on access for legitimate users, which can cause financial losses due to system failures or over-regulation. The development of information security methods is an integral part of adapting to new threats and increasing the resilience of critical systems to cyber threats. Adaptive configuration of the security subsystem should consider the specifics of the subject area, organizational structure and security policy, as mismatching these parameters may cause problems with system availability or security. In case of insufficient attention to security, vectors for attacks can open up, which not only puts data at risk but also causes financial losses due to disruptions in operations. Therefore, the effectiveness of protection is determined by the ability of systems to detect unauthorized actions, adapt to new threats in real-time, and minimize risks, especially in special information systems (SIS), where protection against data modification or destruction is critical [3]. For this purpose, individual threat models and active monitoring methods are used to ensure adequate security in distributed environments [4, 6].

The use of artificial intelligence and machine learning allows for rapid response to threats, the creation of predictive models, and the detection of anomalies, adapting to changes. In addition, the introduction of cyber-physical tools for monitoring components that interact with physical objects, such as industrial systems, energy grids, or smart cities, helps to minimise the risks of large-scale threats to enterprise security.

II. Literature review

An analysis of the current state of information security systems (ISS) reveals serious limitations of existing scientific developments that make it difficult to use them effectively in a dynamically changing cyber environment. The main problems are insufficient consideration of modern trends, such as cloud computing and IoT systems, as well as poor formalisation of the methods underlying the development of information security systems, which makes these systems overly complex and costly for specific threats. The lack of dynamic access control algorithms that take into account user behaviour and the level of threats in real time is another significant problem, especially in the context of adaptive attacks on contextual vulnerabilities of distributed systems.

Research in the field of information security systems is being actively conducted by scientists [4], who integrate methods for

Yuliia Kostiuk, Bohdan Bebeshko, Natalia Mazur and Karyna Khorolska are with Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine (e-mail: y.kostiuk@kubg.edu.ua, b.bebeshko@kubg.edu.ua, n.mazur@ kubg.edu.ua, karynakhorolska@gmail.com)

Nataliia Kotenko and Tetiana Zhyrova are with State University of Trade and Economics, Kyiv, Ukraine (e-mail: kotenkono@knute.edu.ua, zhyrova@knute.edu.ua)

assessing the effectiveness of information security systems with the latest technologies such as artificial intelligence and machine learning [10-15], as well as [5], who develop risk assessment methods for distributed and hybrid systems. Authors [23] investigate risk modelling in distributed environments to assess the effectiveness of information security systems, and work [20] study adaptive methods for determining protection parameters in the face of changing threat models, focusing on adjusting access and protection levels in real time. Authors [1] analyse contextual vulnerabilities in distributed systems, proposing integrating machine learning algorithms for adaptive access control. In work [16] study the assessment of the effectiveness of information security systems in cloud computing and IoT systems, contributing to the development of models for adapting to changing threats [3, 22], and [14] improve assessment methods by integrating Zero Trust Architecture (ZTA) for continuous verification of system elements.

III. Aims and Objectives of the Study

This study aims to develop advanced methods for evaluating and optimizing the effectiveness of information security in modern distributed environments, focusing on precise risk assessment, threat minimization, and resource allocation. Classical approaches are integrated with machine learning, big data analytics, and AI, while novel metrics such as E_{ROI} (Return on Investment in Security) and E_{ROA} (Return on Attack) measure cost-effectiveness and vulnerability. Threat and resource decomposition methods prioritize critical system elements, and Bayesian analysis, risk modelling, and hierarchical analysis enable more accurate attack prediction. By embedding adaptive security frameworks into business processes and balancing confidentiality, integrity, and availability, the proposed models provide flexible, cost-effective protection for uninterrupted and resilient digital operations.

IV. Methods and Models

In the digital era, information security research is based on a systematic approach that includes integrated data protection methods, such as analysing information flows to model their behaviour and select effective security tools, as well as applying probability theory to predict attacks and risks affecting business processes [6, 11]. Methods of discrete mathematics and formal logic help to develop access control algorithms and evaluate the effectiveness of protection, and mathematical modelling is used to evaluate attack scenarios during design. Optimisation of the choice of security tools is carried out using decision theory and multi-criteria optimisation [7, 9-13].

The use of cryptography, intrusion detection and attack blocking systems provides a high level of security, complemented by ISO/IEC 27001 standards [6-8]. Formal assessment methods combined with expert approaches take into account the specifics of particular systems, and the integration of artificial intelligence and machine learning improves data analysis, the creation of predictive models, and dynamic protection settings depending on threats [20-23, 25]. An interdisciplinary approach that combines cybersecurity, economics, and management allows for the creation of adaptive protection systems, minimising their negative impact on the productivity of business processes [18, 19].

V. Computational Experiment

An analysis of the current state of the theory and practice of applying protection mechanisms has revealed the need to create new methodological approaches to assessing the effectiveness of information security systems. This includes analysing the goals and possible attacks by an intruder, as well as developing new approaches to modelling threats and selecting appropriate protective measures. The increased complexity and diversity of threats faced by modern specialised information systems require the use of the latest methods for assessing the level of security based on big data, machine learning and artificial intelligence algorithms [2].

The relevance of developing methods for assessing the effectiveness of information security systems (ISS) for security management in distributed Specialised Information Systems is due to the development of technologies and the complexity of cyber threats, which require improved approaches to ensuring an adequate level of protection in the face of constant changes in threats. The analysis revealed the need for new methodological approaches to assessing the effectiveness of information security systems, including threat modelling, selection of protective measures and analysis of attacks using big data, machine learning and artificial intelligence.

Evaluation of approaches to building secure specialised information systems allows to identify interconnections between methods of risk analysis, damage assessment and selection of protective measures, which is the basis for the development of adaptive and cost-effective information security systems capable of responding to new threats in real time. Methodological approaches should take into account threat forecasting using modern technologies for data analysis, as well as ensure the adaptability of protection systems that change parameters depending on the level of threat. The development of multidimensional risk assessment models should integrate the probability of a threat and its impact on the strategic goals of an enterprise, ensuring effective interaction between information security systems and business processes [2-5, 15] (Fig. 1).

Consideration of various scenarios of unauthorised access threats (UATs) allows one to consider all possible technological barriers and ways to overcome them. In particular, it is important to use models that simulate attacks in real time, which allows one to identify the exact weaknesses in the information security systems. The process of analysing such scenarios can be represented as an attack implementation graph, where each node represents a separate stage of the attack, and each link between them shows the sequence and dependence of the intruder's actions.

Modern approaches to modelling attacks and protecting information systems include machine learning methods for analysing big data and predicting potential threats. The use of such technologies makes it possible not only to determine the likelihood of attacks but also to adapt the information security systems to new conditions, including taking into account rapidly changing factors, such as improved attack methods by intruders, as well as changes in the technical and organisational conditions of the enterprise.

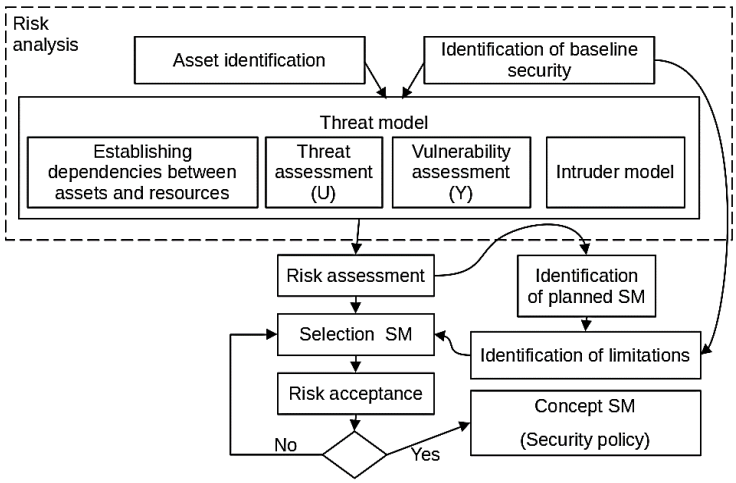

Fig. 1. Scheme of information security system formation

The development of methods for assessing the effectiveness of information security systems for Specialised Information Systems requires innovative approaches that take into account technological, economic and organisational aspects in the context of cyber threats [1]. The existing classification focuses on data confidentiality, but for some Specialised Information Systems, unauthorised actions such as blocking or denial of service are more critical. Traditional methods do not always meet the goals of the system, limiting their effectiveness. Another drawback is the mismatch between threats and regulatory requirements, as well as the subjectivity of assessment methods. For the ISS to work effectively, it is necessary to use risk assessment models, integrating modern methods such as machine learning and big data analysis to improve protection efficiency and predict risks. Threat modelling and evaluation of protection mechanisms are the basis of effective information security systems, and machine learning allows systems to adapt to new attacks [2-5, 7-8].

A fragment of the attack graph annotated with countermeasures and performance indicators is an important tool for modelling and analysing the security of information systems [9] (Fig. 2).

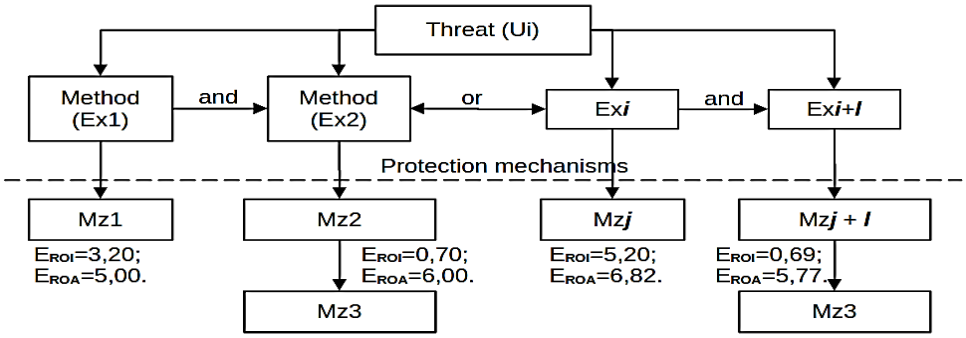

Fig. 2. Fragment of the attack graph annotated with countermeasures and performance indicators

In this context, E_{ROI} (Return on Investment in Security) reflects the effectiveness of the costs of implementing countermeasures aimed at ensuring information security. This indicator takes into account the costs of implementing security measures and compares them with the results achieved, in particular, reducing the likelihood of a successful attack or minimising potential losses. At the same time, E_{ROA} (Return on Attack) reflects the effectiveness of the attacker's actions, including the costs of overcoming the system's defence mechanisms and the benefits gained from a successful attack, and helps to assess the attractiveness of the information system to the attacker in terms of costs and potential benefits. The attack graph annotation allows one to visually show the relationship between the stages of an attack, the probability of its implementation, and the effectiveness of countermeasures. Each vertex of the graph represents a stage of the attack, and the edges represent possible ways to achieve the goal. For each stage, the available countermeasures, their cost and impact on E_{ROI}, as well as the complexity and potential gain for the attacker, which determines the E_{ROA} value, are indicated. This approach makes it possible to assess the effectiveness of security measures and optimise resources to improve cybersecurity [1-2].

The E_{ROI} calculation allows you to make informed decisions about the feasibility of specific security expenditures and assess the cost-effectiveness of implemented solutions. For example, if reducing the likelihood of an attack avoids significant losses and the cost of countermeasures is acceptable, the system is considered effective.

E_{ROA}, in turn, assesses the economic attractiveness of an attack for attackers. This indicator takes into account the costs of organising an attack, including overcoming security mechanisms, and the expected benefits of a successful attack, such as access to critical information or the possibility of its further monetisation. The use of E_{ROA} helps to identify weaknesses in the system that may encourage attackers. The

lower this indicator, the less profitable it is for an attacker to attack a particular information system [3-4].

Taken together, these indicators strike a balance between an enterprise's security costs and the risks posed by an information system in the context of attacks. For example, a high E_{ROI} and low E_{ROA} indicate the effectiveness of security measures and a low probability of attacks, while a low E_{ROI} and high E_{ROA} may indicate deficiencies in the security strategy that should be addressed immediately. Thus, the integration of E_{ROI} and E_{ROA} into information security management processes allows creating adaptive, cost-effective protection systems that meet modern challenges and ensure the stability of distributed information systems [5-6].

The research has led to the conclusion that a numerical assessment of objective indicators of security and the likelihood of threats can be obtained by applying a combined method, when the issues under study are analyzed comprehensively. Since a specialized information system is created to solve specific problems, it is obvious that its potential capabilities must meet the requirements of the scope of the tasks. Therefore, in specific situations, assessment algorithms may differ significantly, which leads to the fact that the application of known methods directly depends on the input data and, for an objective assessment, requires taking into account the entire set of possible ways to overcome obstacles, which should be specified either explicitly as a listed set or as a set of rules that allow the method of influence to be attributed to the set of realized threats. The composition of these sets is determined by experts and needs to be formalized, since a direct search and obtaining the full working space of possible ways to overcome obstacles and foreseeable events lead to the intractability of this set, and its simplification may lead to a loss of adequacy. Thus, the problem of computability is related to the fact that it is impossible to list the entire set of required indicators and assess their adequacy within a reasonable decision-making time.

In this regard, with an increase in the number of estimates, the real probability distribution of possible alternatives is often replaced by some a priori distribution obtained through analysis and expert estimates, which are replete with a large number of ‘taste’ preferences and, therefore, are subjective [14, 18-20, 24-28]. Also, the existing models do not allow for an adequate and complete description of the information processes occurring in distributed computing networks, as a detailed development of aspects of network behavior at different levels of operation is required. In addition, there is no single model that comprehensively covers the three main areas of security—confidentiality, integrity, or availability—each of which is intended for use in a particular aspect of protection.

At the same time, the simultaneous application of different models often leads to conflicting requirements, such as the Biba and Bell–LaPadula models. The Biba model focuses on ensuring data integrity by establishing rules that prevent the level of trust in information from decreasing during its processing. The Bell–LaPadula model, on the other hand, aims to ensure confidentiality by preventing unauthorized access to information and its leakage [11-19, 22-23]. These approaches have different goals and emphasis, which can lead to conflict in systems where it is necessary to ensure a high level of both integrity and confidentiality at the same time. For example, the Biba model’s requirement to prohibit writing information at a lower level of trust contradicts the principle of ‘unreadability from above’ in the Bell–LaPadula model, which aims to restrict access to information at higher levels of secrecy.

Such contradictions require the development of flexible approaches or compromise solutions that balance these requirements. This may include developing specialised access policies, integrating new security models, or using additional mechanisms to resolve conflicts between models [7-13].

The above problems are proposed to be solved by approximating the set of possible solutions by a certain subset that is solvable and then further evaluating the effectiveness with respect to this subset. This approach significantly reduces the requirements for the preliminary analysis of ways to overcome obstacles that are adequate for a particular system and, as a result, allows for achieving sufficiency criteria for modelling threats and assessing their impact [3, 24]. Modern security methods combine classical approaches with new technologies to reduce risks and improve response to threats. Risk assessment and threat forecasting models are key to reliable protection. The numerical assessment is based on a combined method that takes into account the tasks of the Specialized Information System. A priori distributions based on expert opinions can be subjective, and existing models do not always correctly describe processes in networks. To solve these problems, flexible solutions with sufficiency criteria for threat modelling are needed. The use of machine learning and big data analytics improves the accuracy of threat assessment. Assessment through probabilistic calculations contradicts the ISO/IEC 27001 standards [3-5, 16-18], while threat modelling allows for the creation of ISO/IEC 27002-compliant security systems, taking into account dynamic aspects for more accurate threat prediction [9, 12] (Fig. 3).

This makes it possible to present the security policy of a specialised information system formally, using security models, without a detailed consideration of their implementation, which, unlike the informal approach, eliminates the need to operate with complex objects for further analysis.

In the previously considered models, the dependence of the event hazard factor (Kgi) on the damage (gi) caused by the destructive effect of the event (Edi) was accepted. At the same time, the criterion for the level of confidentiality (secrecy) is also the damage (G) arising from the disclosure of information that exceeds the permissible value. Since in the event of a destructive event, the damage occurs regardless of the costs invested in the information security system (ISS), it can be assumed that Kgi will always be constant and equal to 1, i.e. gi in all cases is a constant value that depends only on the value of Edi - 1 or 0. This is logical, since at the time of creation of the ISS, the main task is to neutralise or significantly complicate the implementation of the destructive action, the value of gi of which determined the need for protection measures [21-23].

The concept of efficiency is directly related to the effectiveness of the system, which is expressed in the ratio of useful end results of its functioning to the resources expended. Thus, efficiency acts as an integral indicator at different levels, determining the final characteristic of the system functioning, and, in particular, the efficiency of an information system (IS) indicates the ratio of the characteristics of the effectiveness of its functioning to the costs necessary to achieve these results [13-17, 24].

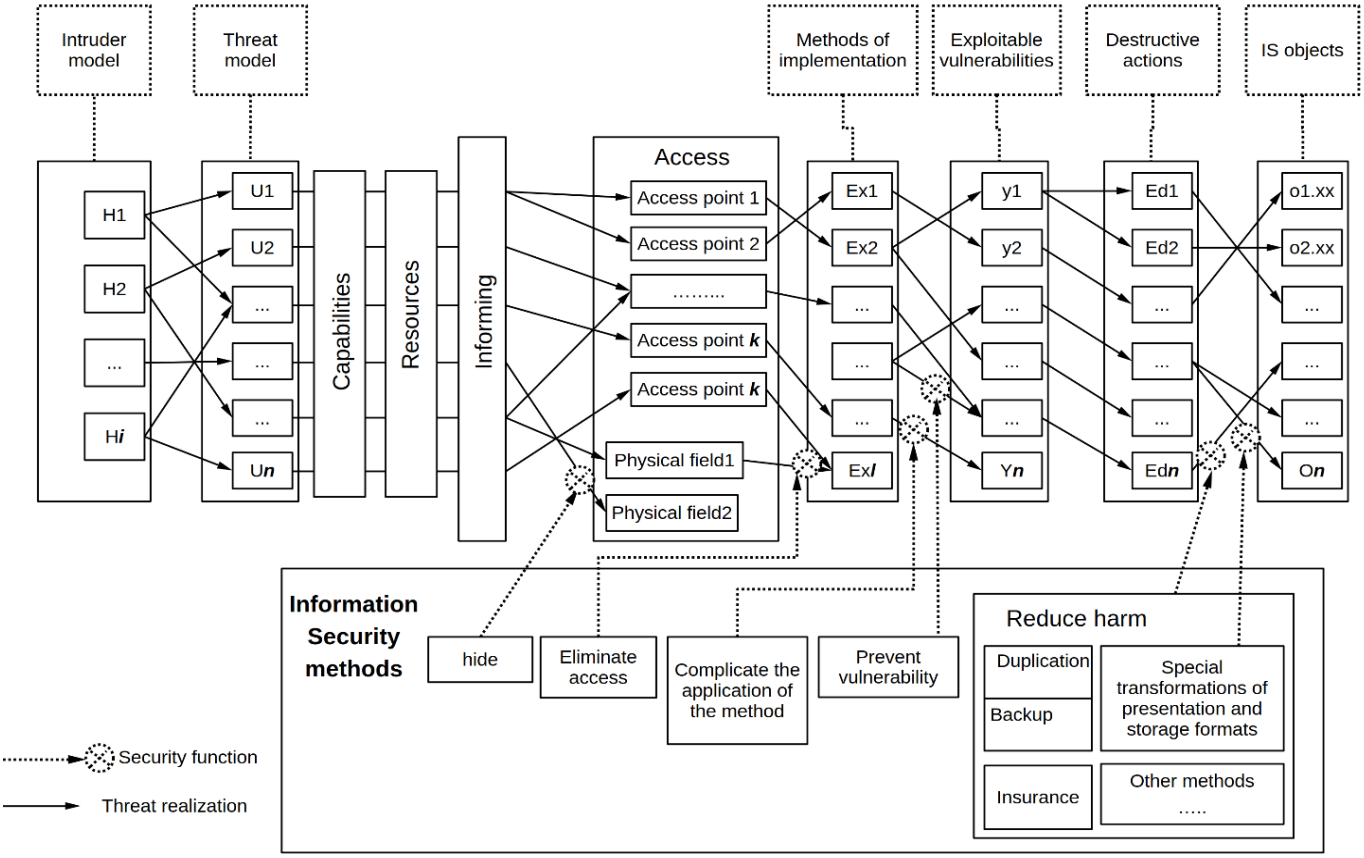

Fig. 3. The 'design' of protection, which determines the relationship between the scheme of threats and methods of their neutralisation

When creating an ISS, the main task is to neutralise or complicate destructive actions, which determines the need for protection. Protection measures lose their meaning when their costs approach the cost of damage from a security breach or when information is no longer secret but still protected, while ignoring the importance of other security aspects, such as integrity or availability [1-4, 11]. Efficiency depends on the effectiveness of the system, which is determined by the ratio of useful results to the resources spent, and the effectiveness of the IS is determined by the ratio of the effectiveness of its functioning to the costs of achieving these results. From the above, it can be concluded that when Edi occurs, the resources spent on building information security systems ($Cz(x)$), are also taken into account as damage (G), since the ISS has not fulfilled its functions. In this case, the main coefficient of ISS efficiency is the indicator of its approximation to the marginal cost of ISS (MCz) [6, 14, 18].

Modern methods of assessing the effectiveness of information security systems also include the use of advanced approaches such as big data analysis and machine learning, which allows for a more accurate assessment of the effectiveness of protection in the face of constantly changing cyber threats [4, 20, 24-25].

$$Kez = \frac{Cz(x)}{MCz}, \quad (1)$$

$$MCz = Cz(x) + R, \quad (2)$$

$$R = Ps(Edi) \times K_g, \quad (3)$$

Where R is the risk of damage remaining after the implementation of ISS measures, $Ps(Edi)$ is the probability of destructive events, and $K_g = 1$.

Because in specialised information systems (SIS), in addition to the threats posed by intruders, we deal with private characteristics, the improvement of which cannot be achieved without deterioration of other partial criteria (e.g. reliability and cost, security and performance), the criterion of effectiveness of such systems is the achievement of a state called 'Pareto Optimality' or Nash equilibrium [6, 14].

Any efficiency criterion can be considered an indicator, but not every indicator should be considered an efficiency criterion. Different indicators characterise the system in different ways. Obviously, the indicators that express the objective function and, therefore, influence decision-making should be chosen as performance criteria. In particular, the MCz value is mainly typical for calculating the Eec (efficiency of effective control) indicators - the effectiveness of the protection system, which is an important aspect when assessing the costs of building an information security system and its effectiveness in the face of constant cyber threats and changing security requirements. Modern approaches to assessing the effectiveness of ISS include not only traditional economic and technical indicators but also the integration of intelligent technologies to predict potential threats and optimize resources [16-19, 21-22, 25].

For systems that are not related to profit, but to the risks of their operation, efficiency directly depends on the damage-cost indicator Euc (effectiveness of unauthorised control) - the effectiveness of the intruder's actions in influencing the system.

That is, if we cannot reduce our own damage (G) with the help of ISS, then we can increase the intruder's costs and risks of a destructive event (Edi). In other words, the most effective system will be the one in which the lowest costs for its protection require the highest costs for its attack [9-10, 23-26].

To evaluate this definition, the Lanchester Model (or CONCOM from Conventional Combat) was chosen, which describes the interaction of resources of the protected system and the attacker. The basic equation of the model is as follows [7]:

$$by^2 - cx^2 = K, \quad (4)$$

Where $K = 2C$ - integration constant; x - resources of the protected system; y - resources of the intruder; b - efficiency of resource use by the intruder; c - efficiency of resource use by the protected system; $b, c > 0$ - proportionality coefficients of the introduced condition; x and y describe the state of efficiency of the protection system (Eec) and efficiency of the intruder's actions (Euc) at the initial time t. The constant K depends on the ratio of the initial resources of the protected system and the intruder. At the initial time t_0 [13]:

$$x = x_0, y = y_0, \quad (5)$$

The integration constant is defined as:

$$K = by_0{}^2 - cx_0{}^2, \quad (6)$$

The model allows you to assess the effectiveness of system protection and predict the state of confrontation based on the ratio of resources: if $by_0{}^2 > cx_0{}^2$, the advantage is on the side of the intruder; if $by_0{}^2 < cx_0{}^2$, the advantage is on the side of the protected system. This equation can also be used to estimate the resources required to achieve a certain level of protection Eec, or to model possible attack scenarios and system responses.

The assumption is made that the defence and attack potentials are proportional according to a certain law $Cx = by$ and $Cy = cx$; while by and cx can also be interpreted as loss rates that depend on the number and intensity of attacks, as well as on the vulnerabilities of the ISS, respectively, b and c are loss and damage coefficients.

Then, when $K = 0$, the efficiency of using the resources of both parties is proportional, since they are reduced and depleted at the same time (final state (0,0)); when $K > 0$, the resources of x are depleted first, i.e. y has an advantage, and when $K < 0$, the resources of y are depleted first, i.e. party x uses its resources more efficiently.

Performance criteria should be related to the objectives of the information system, depend on controllable factors and be easy to interpret. A multiple criterion can be replaced by a single criterion if it is the main one to maximise or minimise, for example, increasing the probability of protection and reducing costs. Modern assessment methods integrate machine learning and forecasting, which allows for more accurate risk prediction and adaptation of protection to new threats, reducing the likelihood of false positives. However, this can upset the balance of protection, for example, ignoring outdated vulnerabilities can reduce system availability due to false alerts that increase resource consumption and reduce responsiveness. Therefore, criteria should take into account optimality, suitability and adaptability, and assessment methods should include physical modelling, expert judgement and combined approaches to evaluate effectiveness in the face of change and emerging threats. Using the above methods and the current stability of individual elements of the ISS - $S_y^i(t)$, a formula was obtained to calculate the current effectiveness of the information system [14, 19-20].

$$Ke(t) = \frac{\sum_i^j \prod ni \cdot S_y^i(t) \cdot K_y^i(t)}{\sum_i^j \prod ni \cdot S_y^i(t)}, \quad (7)$$

where $\prod ni$ are the total potentials of individual elements, calculated by means of computational tasks of determining the efficiency-threat ratio; $S_y^i(t)$ can be interpreted as the current degree of equipment of these elements with protection mechanisms (Mz), which determines their stability; $K_y^i(t)$ is the current efficiency of management of the elements of the information system (IS).

The main criteria for threats were chosen to be their decomposition, which leads them to the following form: X - theft; K - copying (including loss of unregistered media, removal by means of TCP intelligence equipment); P - disclosure (familiarisation, reading or viewing by an unauthorised person); B - blocking; M - modification; Y - destruction [10, 13]. To analyse the level of danger, threats can be represented as a set of weighting factors ω_i, where each factor corresponds to one of the criteria X, K, P, B, M, Y. Taking into account the impact of each threat, the level of danger can be calculated by the formula:

$$L = \omega_X \cdot X + \omega_K \cdot K + \omega_P \cdot P + \omega_B \cdot B + \omega_M \cdot M + \omega_Y \cdot Y, \quad (8)$$

Where L is the level of danger, $\omega_X, \omega_K, \omega_P, \omega_B, \omega_M, \omega_Y$ are weighting factors determined on the basis of a matrix of pairwise comparisons; X, K, P, B, M, Y are estimates of the significance of the respective threats [7, 12, 22]. This model allows taking into account all possible options for attackers' actions and designing optimal protection measures based on the most critical threats.

To determine the likelihood of an attacker using various means of influencing the information system, the following model of influence was adopted, which is implemented through the management system and is aimed at optimising and coordinating management processes, thereby ensuring an effective response to potential threats (Fig. 4).

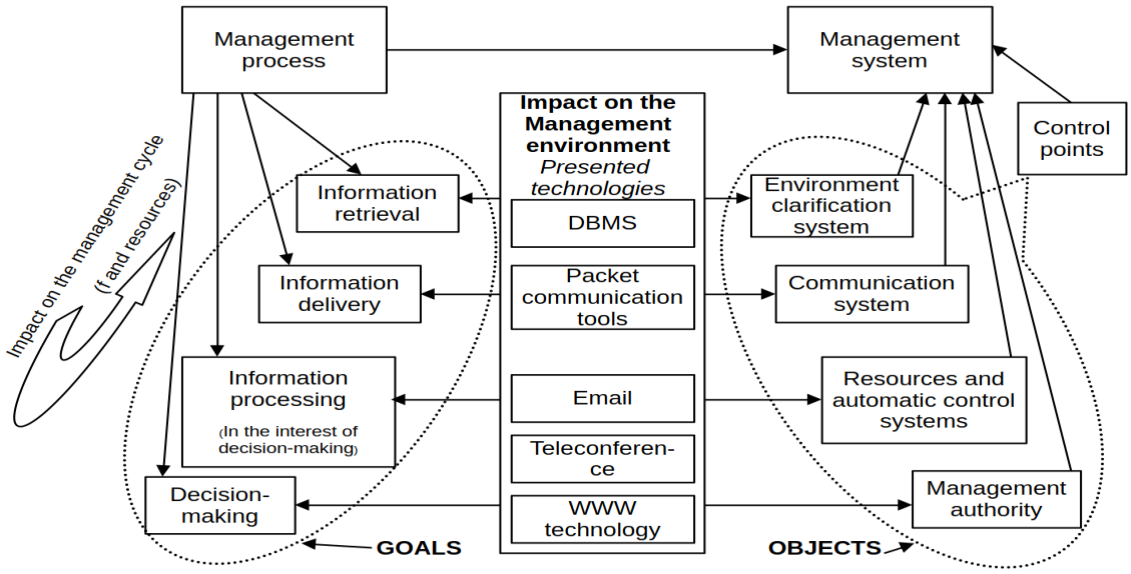

Fig. 4. The model of influence implemented through the management system

The model takes into account technical, organisational and strategic factors that reduce the likelihood of a successful attack and increase the level of system security. Threat assessment in modern security methods should cover all attack options and methods of neutralising them, including the latest information gathering and penetration technologies, such as social engineering and advanced technical hacking tools, which require continuous improvement of protection. The effectiveness of security measures is assessed not only by their ability to neutralise threats, but also by their adaptability to new attacks caused by the evolution of cyber threats, as cybercriminals are constantly improving their methods, creating new attack vectors for which traditional security measures may not be ready [3, 18, 25-26]. In this case, the probability of a threat $P(A)$ can be represented as a complete group of events $H1, H2, \dots, Hn$, which are hypotheses that the attack is carried out using the n-th vulnerability. All events are pairwise incompatible:

$$Hi \cap Hj = \emptyset; j = 1,2, \dots, n; i \neq j, \quad (9)$$

The combination of events forms the space of elementary outcomes Ω:

$$\Omega = H1 \cup H2 \dots \cup Hn, \quad (10)$$

Thus, $H1, H2, \dots, Hn$ form a complete group of events (hypotheses) [4]. Thus, if the event A means that the information system has been successfully attacked ($A \subset \Omega$), the following formula is applied:

$$P(A) = P\left(\frac{A}{H1}\right)P(H1) + P\left(\frac{A}{H2}\right) + \dots + P\left(\frac{A}{Hn}\right)P(Hn), \quad (11)$$

According to the Bayesian formula (for calculating hypothesis probabilities), the probability that an information system will be attacked using the i-th vulnerability is defined as follows:

$$\left(\frac{Hn}{A}\right) = \frac{P\left(\frac{A}{Hn}\right)P(Hn)}{P(A)}; n = \overline{1, i} \quad (12)$$

To obtain a quantitative assessment of the 'Hazard Level', the hierarchy analysis method (MHA) was used with the use of a matrix of pairwise comparisons, which is compiled in accordance with the linguistic rating scale of Thomas Saaty [11]. The following algorithm is used to obtain a quantitative assessment of the 'Hazard Level' using the hierarchy analysis method (MHA), and the following scale is used for the elements of the matrix:

$$A = \begin{bmatrix} 1 & a_{12} & \cdots & a_{1n} \\ \frac{1}{a_{12}} & 1 & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{1}{a_{1n}} & \frac{1}{a_{2n}} & \cdots & 1 \end{bmatrix}, \quad (13)$$

Where A is an $n \times n$ matrix of dimensionality, n is the number of criteria, filled in according to the Thomas Saaty linguistic rating scale, a_{ij} is the assessment of the importance of criterion i relative to criterion j, determined on the basis of expert data.

Normalised weighting coefficients ω_i for each criterion are calculated using the formula [11, 18]:

$$\omega_i = \frac{\sum_{j=1}^{n} a_{ij}}{\sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}}, \quad (14)$$

Where $i = 1,2, \dots, n$. The consistency index (CI) is calculated by the formula:

$$CI = \frac{\lambda_{max} - n}{n-1}, \quad (15)$$

Where λ_{max} is the largest eigenvalue of the matrix A, calculated as:

$$\lambda_{max} = \frac{\sum_{i=1}^{n}(\sum_{j=1}^{n} a_{ij} \cdot \omega_j)}{n}, \quad (16)$$

The consistency index is compared to the random index (RI), the value of which is given by the Thomas Saaty tables. The ratio of the consistency index is called the consistency ratio (CR) and is calculated as follows:

$$CR = \frac{CI}{RI}, \quad (17)$$

If $CR \leq 0.1$, the matrix is considered consistent. Accordingly, for each criterion, its contribution to the overall hazard level is calculated using the formula:

$$L = \sum_{i=1}^{n} \omega_i \cdot \vartheta_i, \quad (18)$$

Where ϑ_i is the value of the i-th criterion. This methodology allows to obtain an objective quantitative assessment of the 'Hazard Level', taking into account the weight of the criteria and the significance of their estimates.

Let the amount of effort required to localise threats be described by the function [18, 22]:

$$G = f\,(R) \cdot t, \quad (19)$$

Where G is the total amount of effort to localise threats (integral assessment); $f(R)$ is a function that depends on the totality of resources, R is material, financial, production, intellectual, labour resources; t is the time required to mobilise and use resources. The resource function $f(R)$ takes into account the contribution of each type of resource to the localisation of threats. It can be detailed as a linear or nonlinear combination of weights for each type of resource:

$$f(R) = a_1 R_m + a_2 R_f + a_3 R_p + a_4 R_i + a_5 R_t, \quad (20)$$

Where R_m, R_f, R_p, R_i, R_t are material, financial, production, intellectual and labour resources, respectively; a_1, a_2, a_3, a_4, a_5 are weighting coefficients characterising the contribution of each type of resource. The time component reflects the efficiency of resource mobilisation. The dependence of G on t is directly proportional, as localisation efforts increase with the delay in resource mobilisation.

In the case of approximate estimates, the function $f(R)$ can be represented as an aggregate sum [22, 25-26]:

$$f(R) \approx k \cdot \sum_{i=1}^{5} R_i, \quad (21)$$

Where k is an integral proportionality coefficient that takes into account the quality of resource management. Then the total amount of effort to localise threats is defined as:

$$G = k \cdot (\sum_{i=1}^{5} R_i) \cdot t, \quad (22)$$

The model can be used to predict the time and resources required to localise specific threats, identify the most resource-intensive stages of protection, and optimise the allocation of limited resources. This helps to increase the efficiency of risk management and reduce the costs associated with information security.

The level of losses associated with threats in an information system can be assessed by measuring the costs required to localise them. For this purpose, the Ki factors corresponding to the main types of threats are used [11, 18, 22-23]:

$$Ki(i =< X, K, P, B, M, Y >) \quad (23)$$

Where i is the type of threat. The Ki factors are calculated by the formula:

$$Ki = \frac{T}{K \times T_\Sigma}, \quad (24)$$

Where T is the time spent on localising a specific type of threat i; K is the number of successful impacts of threat i; T_Σ is the total time spent on localising all threats in the information system. The Ki factors allow us to assess the effectiveness of localising a particular type of threat, the priority of allocating resources to protect against certain threats, and the level of damage that can be associated with each type of threat. Based on these indicators, recommendations can be made to optimise information security, including reallocating resources to reduce the time required to localise critical threats and identifying vulnerabilities that contribute to their successful impact. In this context, the value T_Σ represents the level of damage assessed through the time spent on localising the consequences of an attack on an information system. Then the elements of the matrix of pairwise comparisons will be determined by the value of the ratio:

$$a_{ij} = \frac{Ki}{Kj};\ i =< X, K, P, B, M, Y >, j =< X, K, P, B, M, Y >, \quad (25)$$

Using Bayesian inference, we obtained a probability distribution for the purposes of influencing a specialised information system, which allows us to assess the probability of various threats and select the best measures to neutralise them. The basis of the calculations is Bayes' theorem, which determines the probability of a threat being realised under the existing conditions of observation. The formula for calculating the probability is as follows:

$$P(Threat \mid Observation) = \frac{P(Observation|Threat) \cdot P(Threat)}{P(Observation)}, \quad (26)$$

Where $P(Threat \mid Observation)$ is the probability of a threat occurring given the available observations, $P(Observation \mid Threat)$ is the a priori probability of a threat, $P(Threat)$ is the probability of observation in the presence of a threat, and $P(Observation)$ is the total probability of observation, which serves as a normalisation factor.

To take into account the relationships between threats, information leakage channels, and intruders' actions, a Bayesian trust network was built, which allows predicting the development of events, assessing risks, and optimising protection measures. A method for decomposing threats by type of impact (theft, copying, disclosure, etc.) was developed, taking into account the characteristics of the perpetrators, which allows us to create models for assessing potential threats and adapting protection to new challenges. The Bayesian approach ensures accuracy in risk management, minimising losses to the system. Risk modelling showed that insiders pose the greatest threat, and system optimisation included decomposition of information resources and replacement of expensive security tools with alternative ones, which allows for an increase in security class without increasing maintenance costs.

CONCLUSION

Modern distributed information systems ensure the continuity of business processes and the stability of critical infrastructures, which makes it important to develop effective methods for assessing information security systems for the purpose of accurately assessing security levels, predicting risks and minimising their impact. The main approach is to introduce technologies such as machine learning, big data analysis and artificial intelligence, which provide flexibility and adaptability of protection. The key tools for assessing the effectiveness of information security measures are the E_{ROI} (Return on Investment in Security) and E_{ROA} (Return on Attack) indicators. E_{ROI} reflects the ratio of the cost of implementing countermeasures to the results, such as reducing the likelihood of a successful attack, minimising losses and increasing the level of system security. For example, if the cost of protection is acceptable to avoid significant losses, the system is considered effective. The combination of these indicators allows you to optimise security costs and assess the risks to the system: high E_{ROI} and low E_{ROA} indicate effective protection and low probability of attacks, while low E_{ROI} and high E_{ROA} signal the need to improve the security strategy.

Particular attention should be paid to threat and resource decomposition methods that allow you to optimise security costs by directing them to the most critical elements of the system. Threat and resource decomposition methods allow you to optimise security costs by targeting critical elements of the system, while Bayesian analysis, risk modelling and hierarchical analysis help you to more accurately predict potential attacks, taking into account the specifics of distributed information systems. The integration of adaptive security systems into business processes ensures the cost-effectiveness of security measures, and the balance between confidentiality, integrity and availability of information is achieved through innovative access policies and security models. Thus, effective methods for evaluating security systems for distributed environments are based on integrating classical approaches with the latest technologies, which allows developing adaptive models to improve enterprises' security and stable operation in the digital environment.

REFERENCES

[1] Melaku, H. M. (2023). Context-Based and Adaptive Cybersecurity Risk Management Framework. *Risks*, *11*(6), 101. https://doi.org/10.3390/risks11060101

[2] Gjermeni, Irida & Hoxha, Dudina. (2020). Security and Privacy Methods in Distributed Systems. 10. 59-64. https://doi.org/10.7176/CTI/10-07

[3] Kerimkhulle, S., Dildebayeva, Z., Tokhmetov, A., Amirova, A., Tussupov, J., Makhazhanova, U., Adalbek, A., Taberkhan, R., Zakirova, A., & Salykbayeva, A. (2023). Fuzzy Logic and Its Application in the Assessment of Information Security Risk of Industrial Internet of Things. *Symmetry*, *15*(10), 1958. https://doi.org/10.3390/sym15101958

[4] Kitsios, F.C., Chatzidimitriou, E., & Kamariotou, M. (2022). Developing a Risk Analysis Strategy Framework for Impact Assessment in Information Security Management Systems: A Case Study in IT Consulting Industry. Sustainability.

[5] Xie, P., Dang, Y., & Yang, D. (2021). Research on risk factors of fuzzy evaluation of network security based on computer big data. Journal of Physics: Conference Series, 2033(1), 012171. https://doi.org/10.1088/1742-6596/2033/1/012171

[6] Kostiuk, Y., & Voytkevych, A. (2024). Research on technologies for detecting and identifying violators for corporate network protection. Science and Technology Today (Series "Pedagogy," Series "Law," Series "Economics," Series "Physical and Mathematical Sciences," Series "Engineering"), 4(32), 1017-1032. https://doi.org/10.52058/2786-6025-2024-4(32)-1017-1032

[7] Kostiuk, Y., Bebeshko, B., Kryuchkova, L., Lytvynov, V., Oksanych, I., Skladannyi, P., & Khorolska, K. (2024). 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), 229–252. http://doi.org/10.28925/2663-4023.2024.25.229252

[8] Kostiuk, Y., Skladannyi, P., Korshun, N., Bebeshko, B., & Khorolska, K. (2024). Integrated protection strategies and adaptive resource distribution for secure video streaming over a Bluetooth network. Information Technology, 4(6), 14-33. https://ceur-ws.org/Vol-3826/paper12.pdf

[9] Y. Kostiuk, O. Kryvoruchko, A. Desyatko, Y. Samoilenko, K. Stepashkina and R. Zakharov, "Information and Intelligent Forecasting Systems Based on the Methods of Neural Network Theory," *2023 IEEE International* Conference on Smart Information Systems and Technologies (SIST), Astana, Kazakhstan, 2023, pp. 168-173, https://doi.org/10.1109/SIST58284.2023.10223499

[10] D. Palko, L. Myrutenko, T. Babenko and A. Bigdan, "Model of Information Security Critical Incident Risk Assessment," 2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T), Kharkiv, Ukraine, 2020, pp. 157-161, https://doi.org/10.1109/PICST51311.2020.9468107

[11] Kuzminykh, I., Ghita, B., Sokolov, V., Bakhshi, T. Information Security Risk Assessment. Encyclopedia 2021, 1, 602–617. https://doi.org/10.3390/encyclopedia1030050

[12] Kryvoruchko, O., Kostiuk, Y., Desiatko, A. (2024). Systematization of signs of unauthorized access to corporate information based on application of cryptographic protection methods. Ukrainian Scientific Journal of Information Security, 30(1), 140-149. https://doi.org/10.18372/2225-5036.30.18615

[13] Math, Abdulsattar & Khalf, Mamoon & Abdoon, Fadam & Thivagar, M. (2024). Analysis of Dynamic Systems Through Artificial Neural Networks. Tikrit Journal of Engineering Sciences. 31. 148-158. https://doi.org/10.25130/tjes.31.2.14

[14] Sarker, I.H., Furhad, M.H. & Nowrozy, R. AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions. SN COMPUT. SCI. 2, 173 (2021). https://doi.org/10.1007/s42979-021-00557-0

[15] Min, S., & Kim, B. (2024). Adopting Artificial Intelligence Technology for Network Operations in Digital Transformation. Administrative Sciences, 14(4), 70. https://doi.org/10.3390/admsci14040070

[16] Swapna Siddamsetti & Dr.Rajasekaran Subramanian. Comparative Study of Cyber Security Risk Assessment Frameworks. NeuroQuantology, June 2023, Volume 21, Issue 6, Page 2015-2024. https://doi.org/10.48047/nq.2023.21.6.nq23199

[17] Y. Smitiukh, Y. Samoilenko, Y. Kostiuk, O. Kryvoruchko and K. Stepashkina, "Development of a prototype of an intelligent system for predicting the quality of dairy manufacture," 2022 IEEE 11th International Conference on Intelligent Systems (IS), Warsaw, Poland, 2022, pp. 1-6, https://doi.org/10.1109/IS57118.2022.10019699

[18] A. Alahmari and B. Duncan, "Cybersecurity Risk Management in Small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence," 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), Dublin, Ireland, 2020, pp. 1-5, https://doi.org/10.1109/CyberSA49311.2020.9139638

[19] Umar, D. (2024). Cybersecurity Threats and Mitigation Strategies in the Age of Quantum Computing. Journal of Technology and Systems, 6(5), 1–14. https://doi.org/10.47941/jts.2145

[20] Yang, H., Zhu, J. & Li, J. Cybersecurity and Risk Prediction Based on Machine Learning Algorithms. Applied Mathematics and Nonlinear Sciences, 2024, Sciendo, vol. 9 no. 1, https://doi.org/10.2478/amns-2024-2480

[21] Bakhtavar, E., Valipour, M., Yousefi, S. et al. Fuzzy cognitive maps in systems risk analysis: a comprehensive review. Complex Intell. Syst. 7, 621–637 (2021). https://doi.org/10.1007/s40747-020-00228-2

[22] Erdoğan, M., Karaşan, A., Kaya, İ., Budak, A., Çolak, M. (2020). A Fuzzy Based MCDM Methodology for Risk Evaluation of Cyber Security Technologies. In: Kahraman, C., Cebi, S., Cevik Onar, S., Oztaysi, B., Tolga, A., Sari, I. (eds) Intelligent and Fuzzy Techniques in Big Data Analytics and Decision Making. INFUS 2019. Advances in Intelligent Systems and Computing, vol 1029. Springer, Cham. https://doi.org/10.1007/978-3-030-23756-1_123

[23] F. -H. Liu, "Constructing Enterprise Information Network Security Risk Management Mechanism by Using Ontology," 21st International Conference on Advanced Information Networking and Applications

Workshops (AINAW'07), Niagara Falls, ON, Canada, 2007, pp. 929-934, https://doi.org/10.1109/AINAW.2007.129

[24] Shelly, E. (2024). Cybersecurity Frameworks for Cloud Computing Environments. International Journal of Computing and Engineering, 6(1), 30–44. https://doi.org/10.47941/ijce.2058

[25] Irsheid, A., Ahmad, M., AlNajdawi, M., & Qusef, A. (2022). Information security risk management models for cloud hosted systems: a comparative study. Procedia Computer Science, 204, 205-217. https://doi.org/10.1016/j.procs.2022.08.02

[26] Prerna Patil, Charvi Kumar, Rutuja Kadam, Yatin Gandhi. (2024). An Analysis of Emerging Cybersecurity Threats in Cloud Computing. Computer Fraud and Security, vol.2024 (7). https://doi.org/10.52710/cfs.64

[27] Lakhno, V., Akhmetov, B., Mazaraki, A., Kryvoruchko, O., Chubaievskyi, V., Desiatko, A. Methodology for assessing the effectiveness of measures aimed at ensuring information security of the object of informatization (2021) Journal of Theoretical and Applied Information Technology, 99 (14), pp. 3417-3427. http://www.jatit.org/volumes/Vol99No14/5Vol99No14.pdf

[28] V. Lakhno, V. Malyukov, B. Akhmetov, B. Yagaliyeva, O. Kryvoruchko and A. Desiatko, "University Distributed Computer Network Vulnerability Assessment," 2023 IEEE International Conference on Smart Information Systems and Technologies (SIST), Astana, Kazakhstan, 2023, pp. 141-144, https://doi.org/10.1109/SIST58284.2023.10223501

[29] Lakhno, Valerii; Alimseitova, Zhuldyz; Kalaman, Yerbolat; Kryvoruchko, Olena; Desiatko, Alona; Kaminskyi, Serhii. Development of an Information Security System Based on Modeling Distributed Computer Network Vulnerability Indicators of an Informatization Object. International Journal of Electronics and Telecommunications. Vol. 69, No. 3, pp. 475-483 https://doi.org/10.24425/ijet.2023.146495