Effectiveness of Information Security Control using Audit Logs*

Yuliia Kostiuk[1,†], Pavlo Skladannyi[1,*,†], Volodymyr Sokolov[1,†], Oleksii Zhyltsov[1,†] and Yevhen Ivanichenko[1,†]

[1] *Borys Grinchenko Kyiv Metropolitan University, 18/2 Bulvarno-Kudriavska str., 04053 Kyiv, Ukraine*

Abstract

With the ever-increasing interconnectedness of computers through corporate networks and the Internet, ensuring information security and implementing appropriate security policies and procedures is becoming increasingly important. An essential aspect of security is information registration in security audit logs. At present, information security is ensured through corporate application packages that use security agents specific to each platform. These agents are installed on workstations to provide security, but they have limited capabilities and are only part of the application suite. There is a need to find optimized solutions. When detecting an attack, the proactive audit system makes a decision on neutralization, taking into account the type of object and attack conditions, and performs various measures, such as notifying the administrator, blocking user access, and rebooting the workstation. The general model of proactive audit logs eliminates agents and places security audit logs on a remote server. The server can perform a thorough and intelligent analysis of audit logs to effectively verify and enforce security policies in a more comprehensive format. This paper aims to analyze and study the use of audit logs for security purposes in enterprise products.

Keywords

security audit, information security, audit log, security policy, monitoring, security agents, process model, fuzzy Petri net

1. Introduction

Ensuring information security is a key issue for the stability of business and public infrastructure, which requires continuous improvement of technical security measures that can complicate unauthorized access [1, 2]. The growing use of information technology in the business environment, in particular via the Internet, contributes to the vulnerability of enterprise computer systems, which, in turn, increases the likelihood of unauthorized actions from both inside and outside organizations [3–6]. When analyzing the security of small and medium-sized enterprises, there are difficulties associated with the formalization of requirements and the use of statistics on IS incidents, due to the diversity of system components and the limited public availability of facts about leaks or information security incidents, in particular due to strategic decisions of management to disclose vulnerabilities [7, 8]. This leads to expert assessments, such as scoring systems, introducing uncertainty into the final results, complicating analysis, and decision-making.

An organization's required level of information security is achieved by creating an effective information security system, where a timely and complete assessment of the existing or being developed security system is key to ensuring the availability, integrity, and confidentiality of information assets. For this purpose, it is crucial to know the status, characteristics and parameters of the security mechanisms used, as well as awareness of the level of their compliance with the requirements, which allows identifying weaknesses in the security system and provides an opportunity to improve it through recommendations for modernization [4, 9]. The process of such

CPITS 2025: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, February 28, 2025, Kyiv, Ukraine

* Corresponding author.

† These authors contributed equally.

y.kostiuk@kubg.edu.ua (Y. Kostiuk); p.skladannyi@kubg.edu.ua (P. Skladannyi); v.sokolov@kubg.edu.ua (V. Sokolov); o.zhyltsov@kubg.edu.ua (O. Zhyltsov); y.ivanichenko@kubg.edu.ua (Y. Ivanichenko)

0000-0001-5423-0985 (Y. Kostiuk); 0000-0002-7775-6039 (P. Skladannyi); 0000-0002-9349-7946 (V. Sokolov); 0000-0002-7253-5990 (O. Zhyltsov); 0000-0002 6408-443X (Y. Ivanichenko)

an assessment should be carried out regularly and is called an IS audit, which has been studied by many scientists, including Ziro Aasso, Shara Toybayeva, Azamat Imanbayev, Zhaybergenova Zhanshuak, Y. Xu, Y. Yang, T. Li, J. Ju and Q. Wang, Cheryl Vroom, Solms Rossouw, Edegbeme-Belaz Annamarie, Kerti Andras, Stephen Ganz, Gerat Tejasvini, Gerat Hemanta, Satoh Naoki, Samejima Masaki, Wang Zhanjiang, Wang Shuoning, Wang Ling and others [1–17].

There are various risk assessment and management approaches, including the statistical method, the approach based on expert judgment and subjective probability, the probabilistic-statistical approach, the theoretical-probabilistic method, and the risk calculation method. However, these methods do not always adequately reflect real affairs, since the security system must withstand specific IS threats and destructive actions against information assets. Therefore, there is a need to develop IS audit methods that provide quantitative assessments and meet modern information security requirements [16, 18].

An essential element of ensuring information security is effective information security control, particularly through audit logs that record all actions in computer systems and can be the basis for analyzing security breaches [19, 20]. Each user action must be accurately recorded, contributing to implementing a high-level information technology security policy. Integrating audit logs into corporate product packages is vital in ensuring security and maintaining a proactive approach to information technology security.

In today's information environment, sophisticated enterprise software packages that meet the needs of large enterprises for integrated solutions include application management, business process management, Internet control, network management, workstation and server management, and security. In this context, security management includes security auditing based on checking logs to identify entries that may indicate a security breach. However, this process only partially solves the problem within large software packages, as most such products use similar principles and methods to process logs and identify potential threats.

2. Model of the information security audit process

The functional model of information security audit of an information system is a structured approach that defines the stages, methodology, and criteria for assessing the security system's effectiveness [14, 16, 18, 21]. The process includes planning, information collection, risk assessment, audit, analysis of results, report development, and follow-up. At the planning stage, the audit's goals, objectives, and scope are determined, and an audit consent is formed to conduct the audit. Information gathering involves analyzing documentation, such as security policies and procedures, and interviews with specialists and users to obtain details about the system's operation. Risk assessment involves identifying threats and vulnerabilities that could lead to non-compliance with security requirements. Audit includes technical analysis and verification of technical aspects of security and evaluation of compliance with policies and standards. The report consists of documentation of the results, identified problems, and recommendations for elimination. Upon completion of the audit, the implementation of recommendations is monitored, and preparations are made for further audits to improve the security system [15–17, 22, 23]. The model provides a comprehensive and systematic approach to ensuring the effectiveness of information security of information systems (Fig. 1).

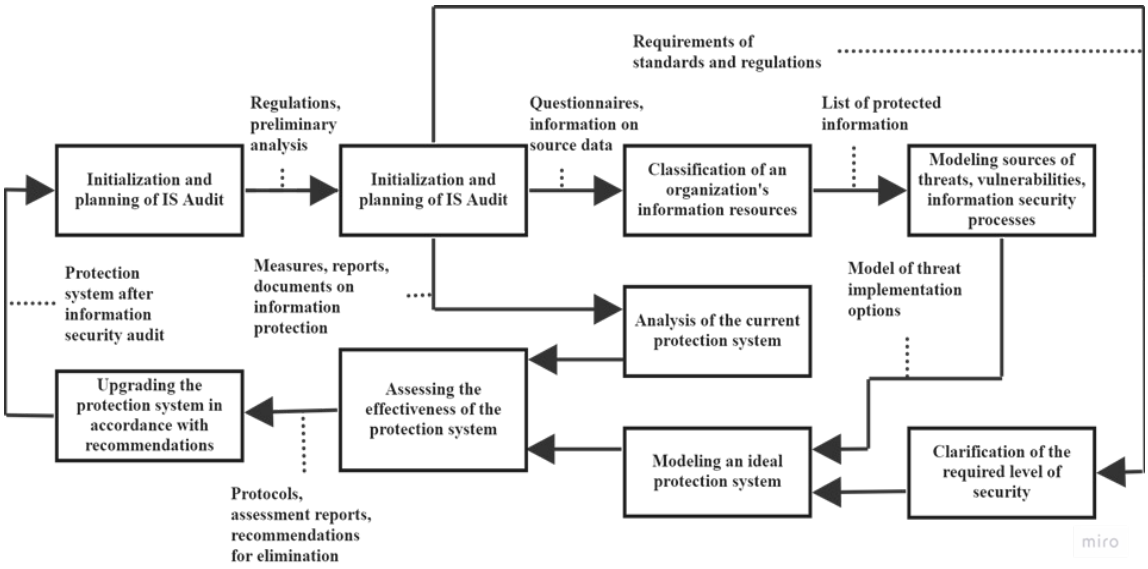

Figure 1: Functional model of the process of conducting an information security audit of an information system

The model reflects the complexity of audit tasks and allows auditors to systematically and effectively assess the degree of compliance of an information system with security requirements. The built functional model is essential for ensuring high security and compliance with information security standards.

3. Methodology for auditing the information security of an information system

The development of an IS audit methodology for modernizing a security system that meets current threats is essential and depends on assessing the effectiveness of such systems. To eliminate the shortcomings of existing methods to evaluate the likelihood of realization of IS threats, which do not take into account the sources of threats and destructive actions against information assets, a new method for assessing the likelihood of realization of threats has been developed that allows taking into account the parameters of threat sources, vulnerable links in the system and their impact on critical assets [15–17, 20, 23–25]. This method improves the accuracy and objectivity of IS threat assessment, considering a wide range of factors affecting security.

An analysis of approaches to detecting internal attacks has revealed significant shortcomings in prototype attack detection systems, complicating their implementation in corporate networks. The problems are the complexity of implementation, the choice of methods for data collection, attack detection, data processing, and load distribution on system components. Traditional methods, such as signature and anomaly detection, do not provide effective attack detection. Neural network-based methods have certain advantages, but suffer from the complexity of setup, high resource requirements, and difficulty in retraining. Therefore, existing approaches do not meet the requirements of effective control over the conduct of an IS audit. Further research should help improve attack detection systems and ensure high security in corporate networks. A promising alternative is the development of active audit systems based on artificial intelligence, which provide high speed, ease of training, and low resource consumption. “Active auditing” is a continuous process of checking the system for compliance with the security policy and automatically responding to deviations [13, 15, 17]. It combines elements of traditional audit and intrusion detection systems, making it an effective tool for IS control. The security state of an information system depends on a set of events occurring in the network. It is described by a fuzzy network called a Petri net, which is used to model and analyze processes related to the control and security of information systems. In particular, a fuzzy Petri net can model the information security

audit process by defining system states, audit-related actions, and their interactions. Audit logs can be represented as one of the system elements. Modeling using fuzzy Petri nets is a powerful tool for analyzing and optimizing audit processes, including the stages of information collection, analysis of audit logs, detection of anomalies, and development of countermeasures. Each is a separate subnetwork with defined transitions marked by audit activities. This approach allows you to identify potential risks, analyze audit effectiveness, and develop optimal control strategies using mathematical methods, which helps to improve security systems and detect threats. For this purpose, a set of information systems states is defined:

$$S=\{S_1,S_2,S_3,S_4,S_5\}, \tag{1}$$

where S_1 is the state of normal functioning of an information system; S_2 is the state of an attack on an information system in which an attacker affects the information system to disrupt its normal functioning; S_3 is the state of violation of the confidentiality of information system resources; S_4 is the state of violation of the integrity of information system resources; S_5 is the state of violation of the availability of information system resources. The set of events in the information system is determined:

$$K=\{K_1,\ldots,K_6\}, \tag{2}$$

where K_1 is the event of an intruder; K_2 is a set of events leading to a breach of confidentiality; K_3 is a set of events leading to a breach of integrity; K_4 is a set of events leading to a breach of availability; K_5 is a set of events that trigger information system security measures; K_6 is a set of events that result in the recovery of an information system after an attack.

A set of events in an information system is a union of sets of events in an information system, i.e.:

$$K=\{K_1\cup K_2\cup K_3\cup K_4\cup K_5\cup K_6\}. \tag{3}$$

A fuzzy Petri net that describes the behavior of an information system has the following form:

$$C_f=(N,f,\lambda,m_0), \tag{4}$$

where N is the structure of the fuzzy Petri net (Fig. 2), $N=(P,T,I,O)$; $f=\{f_1,\ldots,f_u\}$ is the vector of values of the membership function of fuzzy transition triggering, $f_j\in[0,1]$, $j=1,\ldots,u$; $\lambda=\lambda_1,\ldots,\lambda_u$ is the vector of values of transition triggering thresholds, $\lambda_j\in[0,1]$, $j=1,\ldots,u$; m_0 is the vector of initial labeling, $m_l^0\in[0,1], l=1,\ldots,n$.

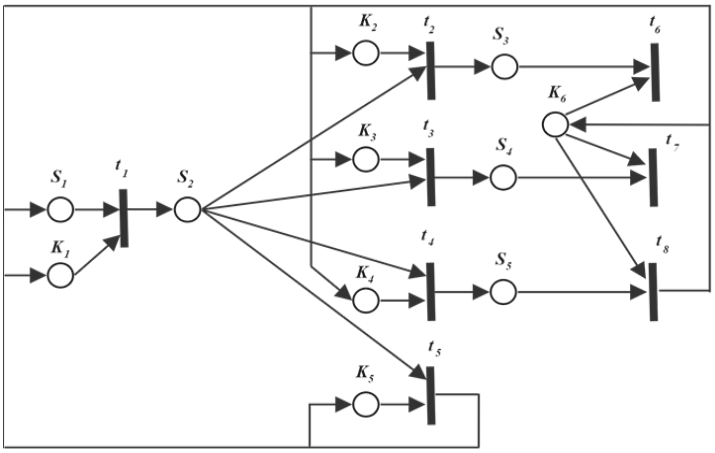

Figure 2: Structure of a fuzzy Petri net

The structure of the fuzzy Petri net $N=(P,T,I,O)$ is similar to the structure of a traditional Petri net and can be represented by the following elements [21]: $P=\{p_l,\ldots,p_n\}$ is a set of positions of a fuzzy Petri net, $T=\{t_1,t_2,\ldots,t_u\}$ is a set of transitions of a fuzzy Petri net, $u\in N$; I is the input function of transitions, $I\,P\times T\rightarrow\{0,1\}$; O is the output transition function, $O\,T\times P\rightarrow\{0,1\}$.

A base of rules for fuzzy inference is formulated, which defines the conditions for triggering the transitions of the fuzzy Petri net. Each predicate from the compiled rules is matched with a particular position of the fuzzy Petri net. Each position of $P=\{p_l,\ldots,p_n\}$ is matched with elements of the sets S and K:

$$P=\{S_1,K_1,S_2,K_2,K_3,K_4,K_5,S_3,S_4,S_5,K_6\}. \tag{5}$$

Next, the initial labeling vector is determined:

$$m_0=\left(m_1^0,m_2^0,m_3^0,m_4^0,m_5^0,m_6^0,m_7^0,m_8^0,m_9^0,m_{10}^0,m_{11}^0\right), \tag{6}$$

where $m_1^0(l=1,3,8,9,10)$ are the values of the membership functions for the presence of markers in positions $S_1\ldots S_5$ that is, the values of the membership functions that determine the different states of the information system, m_2^0 determines the value of the membership function for the presence of a marker in a position K_1, which determines the probability of an intruder in the information system, m_j^0 $(j=4,5,6)$ are values of the membership functions for the presence of markers in positions K_2, K_3, K_4, which leads to a violation of the confidentiality, integrity, and availability of information in the information system, m_7^0 determines the value of the membership function for the presence of a marker in a position K_5, which determines the actual probability of a correct response to an attack by active audit tools, m_{11}^0 is the value of the membership function for the presence of a marker in position K_6, which determines the probability of a correct response of recovery tools after an attack, the values of the membership functions $m_1^0=1, m_{3,8,9,10}^0=0, m_{4,5,6}^0=1, f_{18}=1$ are also accepted.

The dynamics of changing the labels of a fuzzy Petri net are determined by the following rules [21]:

1. The rule for determining the current marking any state of the fuzzy Petri net is determined by the vector m , whose components are interpreted as the value of the membership function of the presence of one marker in the corresponding positions of the fuzzy Petri net.
2. The rule of active transition $t_k\in T$ of a fuzzy Petri net is active if the condition is met:

$$\min\{m_l\}\geq\lambda_k;(t\in\{1,2,\ldots,n\})\wedge(I(p_l,t_k)>0). \tag{7}$$

3. Rule for fuzzy triggering of transition, if transition $t_k\in T$ of the fuzzy Petri net is active, then fuzzy triggering leads to a new labeling m^v, whose vector components are determined as follows:

$$\begin{gathered} m_l^v=0,(\forall\, p_l\in P)\wedge\left(I(p_l,t_k)>0\right), \\ m_j^v=\max\{m_j,\min\{m_l,f_k\},(\forall\, p_l\in P)\wedge(I(p_l,t_k)>0)\}, \\ i\in\{1,2,\ldots,n\}\wedge\left(I(p_l,t_k)>0\right). \end{gathered} \tag{8}$$

During the initial markup, the t_1 link is active when:

$$m_2^0\geq\lambda_1, \tag{9}$$

i.e., if the probability of an attacker is greater than the threshold of the transition t_1. Next, we analyze the following transitions in the information system. If condition (9) is satisfied, then the fuzzy triggering of the transition t_1 will lead to a new labeling m_1. At the same time $m_1^1=m_2^1=0$,

since the positions S_1 and K_1 are input values for the transition. For the position $S_2 \cdot m_3^1 = max\{0, min\{m_2^0, 1\}\}$, i.e., $m_3^1 = m_2^0 \geq \lambda_1$. All other positions remain unchanged, since $m_{4,5,6}^1 = 1$, then the transitions t_2, t_3, and t_4 will be active when the conditions $m_3^1 > \lambda_2, m_3^1 > \lambda_3, m_3^1 > \lambda_4$. Transition t_5 will be active when the condition is met:

$$\min\{m_3^1, m_7^1\} > \lambda_5 \text{ or } \min\{m_2^0, m_7^0\} > \lambda_5. \quad (10)$$

The analysis of expressions (9) and (10) indicates that achieving secure operation of the information system is possible by: (a) increasing the value of the coefficient λ_1, which can be achieved by properly setting up the IS security policy; (b) reducing the value of the coefficient λ_5, which is the threshold of sensitivity of the active audit system. In addition, it is necessary to work on increasing the value of the coefficient m_7^1.

The structure of the active audit system (Fig. 3) includes sensors for analyzing and processing information about the functioning of the information system and user actions, a database for storing the received information, a data analysis and processing unit for streaming input data and generating control actions, a response unit that affects the information system, an administrator console, and a log of the active audit system.

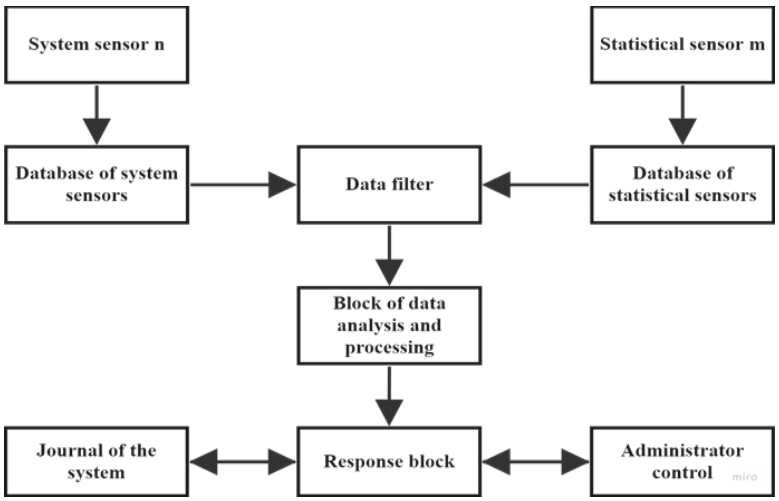

Figure 3: Flowchart of active audit

System sensors analyze system parameters and user actions, generating alerts for further processing, detecting attempts to brute force passwords, mount media, and log in/out, and statistical sensors generate profiles to record typical behavior. The data filter eliminates duplicate alerts, increasing system efficiency. To improve signal processing, it is necessary to ensure reliable storage of incoming information, fast signal processing for prompt detection of attacks and timely decision-making, as well as secure storage of information for updating user profiles, using encryption and data protection, which will increase the efficiency of the active audit system [13, 15, 17, 20, 22–25].

The signature method, which is effective for known threats, and the neural network method, which is capable of detecting new attacks but requires customization and significant computing resources, are used to detect abnormalities. If an attack is detected, the active audit system makes a decision based on fuzzy logic, considering the type of object and attack conditions, with the option of notifying the administrator, blocking access, rebooting the workstation, or unloading programs.

Critical information resources are initially identified, each of which is assigned importance labels regarding confidentiality, integrity, and availability of information. The threat analysis algorithm includes identifying potential threats, classifying them, creating an attacker model, identifying protection methods, and assessing the level of security. After which, the possible damage and probability of the threat being realized are evaluated, allowing for the creation of a threat model for a particular organization. This approach ensures systematic threat management and prevention of negative consequences.

The threat realization rate Y indicates whether a specific threat will be realized in a given system, taking into account the probability of the danger being discovered and the level of initial protection of the valuable asset targeted by the threat. The formula calculates it:

$$Y = \frac{(X + K)}{2}, \tag{11}$$

where Y is a threat realization, $0 \le Y \le 10$; X is the probability of information security threats realization, $0 \le X \le 10$; K is the level of initial security of a valuable asset, $0 \le K \le 10$.

The information security risk level R means the probability of a particular adverse event associated with the realization of a specific threat, which has a certain probability of occurrence and can lead to potential damage. When calculating this indicator, it is vital to take into account three parameters and use a special formula:

$$R = Z \cdot \frac{Y \cdot U}{10}, 0 \le R \le 100, \tag{12}$$

where U is the magnitude of the vulnerability; Y is the realization of threats; Z is the damage from the realized threat. Once a risk is identified, it is essential to consider ways to mitigate it. There are five primary methods: risk avoidance, risk transfer, risk reduction, radical risk reduction, and risk acceptance.

It is possible to assess an organization's information security level only if you calculate the value of several risks or risks for a particular block. For example: by security areas, by information security measures, by valuable assets (employees of the organization). To determine the level of information security of an organization by a block of parameters, it is necessary to:

$$R_{\text{total}} = \frac{1}{n} \sum_{i=1}^{n} R_i, \tag{13}$$

$$O_j = 1 - \prod_{i=1}^{n} (1 - O_{ij}) \tag{14}$$

where O_{ij} is the probability of occurrence of the i^{th} threat source in the interests of realizing the j^{th} threat, n is the number of threat sources that can realize the j^{th} security threat.

Vulnerable links between the information system and its relationship with the considered IS threats have been identified. The list of potential vulnerable links is determined based on the developed questionnaires. The probability of exploitation of the vulnerable link characterizes each vulnerable link. The relationship between vulnerable links and IS threats, based on the information in the information security threat database, makes it possible to determine the likelihood of exploiting vulnerable links in the interests of implementing the j threat:

$$V_j = 1 - \prod_{k=1}^{m} (1 - V_{kj}), \tag{15}$$

where V_{kj} is the probability of exploiting the k^{th} vulnerable link in the interests of implementing the j^{th} threat, m is the number of vulnerable links through which the j^{th} security threat can be implemented.

The destructive actions against critical information resources of the information system and the probability of performing a specific destructive action based on the degree of importance of the information system resources are determined [17, 19, 23, 24]. Each identified possible IS threat is matched with destructive actions that may result from its implementation. The relationship is based on analyzing information in the database of information security threats. The probability of performing destructive actions against the$r$ information asset as a result of the implementation of the j threat as a result of the implementation of the j threat is calculated by the formula:

$$D_{rj} = 1 - \prod_{j=1}^{l} (1 - D_{grj}), \tag{16}$$

where D_{grj} is the probability of performing the g^{th} destructive action during the implementation of the j^{th} agrozone with the r^{th} information resource, l is the number of harmful actions that will result in the j^{th} security threat.

The same threat can be implemented against different information assets of an information system. At the same time, it is considered realized if at least one destructive action has been performed. Therefore, knowing the probability of each threat being discovered to each information asset is necessary. Since the events that lead to the realization of IS threats are independent, the probability of a security threat to the$r$ information asset is calculated using the probability of the product of events formula:

$$P_{rj}=O_j \cdot V_j \cdot D_{grj}. \quad (17)$$

The probabilities of security threats to$r$ information assets form a complete group, so the total probability of a particular threat is calculated using the formula of total or average probability:

$$P_j=\sum_{r=1}^{t} P_{rj} \cdot \frac{1}{t}, \quad (18)$$

where t is the number of information assets to be protected in respect of which the j^{th} IS threat may be realized in respect of which thej^{th} IS threat may be realized.

To evaluate the security system's effectiveness, it is necessary to assess its efficacy against each current threat based on the measures taken to minimize the likelihood of this IS threat being realized [15–17, 20, 22, 23]. The assessment will be based on the adequacy of measures that compensate for the IS threats. The result of the study of ways to assess the effectiveness of the protection system was the development of a method for determining the effectiveness of the ISMS based on the Mamdani fuzzy inference system.

For this purpose, each input and output variable is described as a linguistic variable in a formalized form. The following variables are used:

For this purpose, each input and output variable is described as a linguistic variable in a formalized form. The following variables are used (Fig. 4):

1. β_x is "Threat probability" (probability of realization of an actual security threat) with the scope of definition $X=[0,100]$ and a set of base values

$$T_x=\{\text{very low}, \text{low}, \text{medium}, \text{high}, \text{very high}\}=\{a_{x1}, a_{x2}, a_{x3}, a_{x4}, a_{x5}\}.$$

2. β_y is "Compliance of measures" (compliance of measures to compensate for the IS threat) with the scope of the definition $Y=[0,100]$ and a set of baseline values

$$T_x=\{\text{practically absent}, \text{small}, \text{moderate}, \text{high}, \text{very high}\}=\{a_{y1}, a_{y2}, a_{y3}, a_{y4}, a_{y5}\}.$$

3. β_z is "Protection system effectiveness" (Assessment of the effectiveness of the protection system) with the scope of the definition $Z=[0,100]$and a set of baseline values

$$T_x=\{\text{not effective at all}, \text{insufficiently effective}, \text{moderately effective}, \text{effective}, \text{very effective}\}=$$
$$=\{a_{z1}, a_{z2}, a_{z3}, a_{z4}, a_{z5}\}.$$

Membership functions are built for each of the variables. Trapezoidal functions built based on expert opinions are used as membership functions (Fig. 4).

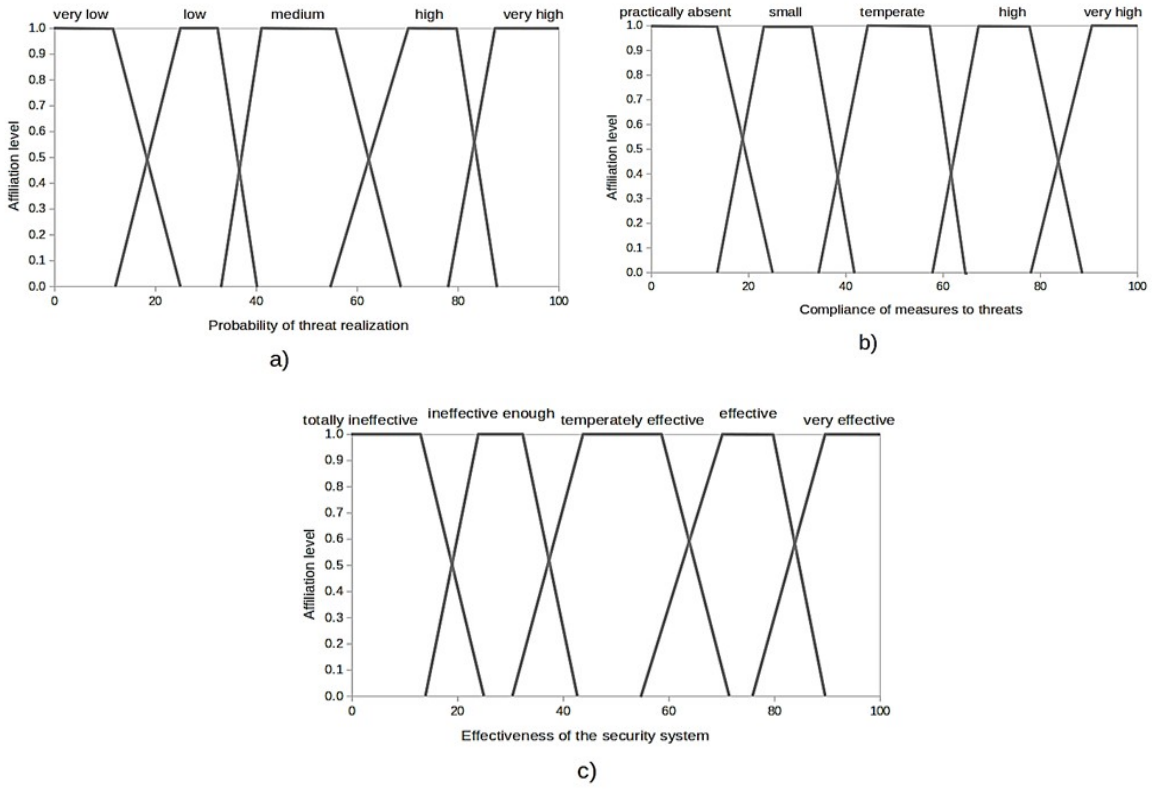

Figure 4: Graphs of functions of linguistic variables (a) "Probability of threat," (b) "Appropriateness of measures," and (c) "Effectiveness of the protection system"

Fuzzy rules reflecting the relationship between input and output parameters are formed. Such statements are presented as a matrix of positioning the effectiveness of the protection system (Table 1).

Table 1
Matrix for positioning the effectiveness of the protection system

	a_{y5}	a_{y4}	a_{y3}	a_{y2}	a_{y1}
a_{x5}	a_{z4}	a_{z4}	a_{z3}	a_{z2}	a_{z1}
a_{x4}	a_{z4}	a_{z4}	a_{z3}	a_{z2}	a_{z1}
a_{x3}	a_{z5}	a_{z4}	a_{z3}	a_{z3}	a_{z2}
a_{x2}	a_{z5}	a_{z5}	a_{z4}	a_{z3}	a_{z2}
a_{x1}	a_{z5}	a_{z5}	a_{z4}	a_{z3}	a_{z2}

The input values of the linguistic variables are located vertically and horizontally, and the output variable values are located at the intersection. The graphs of membership functions and fuzzy rules form a knowledge base that allows using the Mamdani fuzzy inference method to obtain a quantitative output variable value. It is advisable to implement it in the MATLAB environment using the FUZZY LOGIC package, which makes it possible to evaluate the effectiveness of the protection system according to two specified input parameters [3, 8–11, 15–17, 19, 23, 25].

An information security audit of an information system is conducted in the following sequence: collecting initial data and describing the object of protection, identifying critical resources, sources of threats and their probabilities, identifying vulnerabilities and their connection with current threats, assessing destructive actions against information assets and the likelihood of threats, evaluating protection measures and the effectiveness of the protection system for each threat, and formulating recommendations for improving the protection system by regulatory requirements.

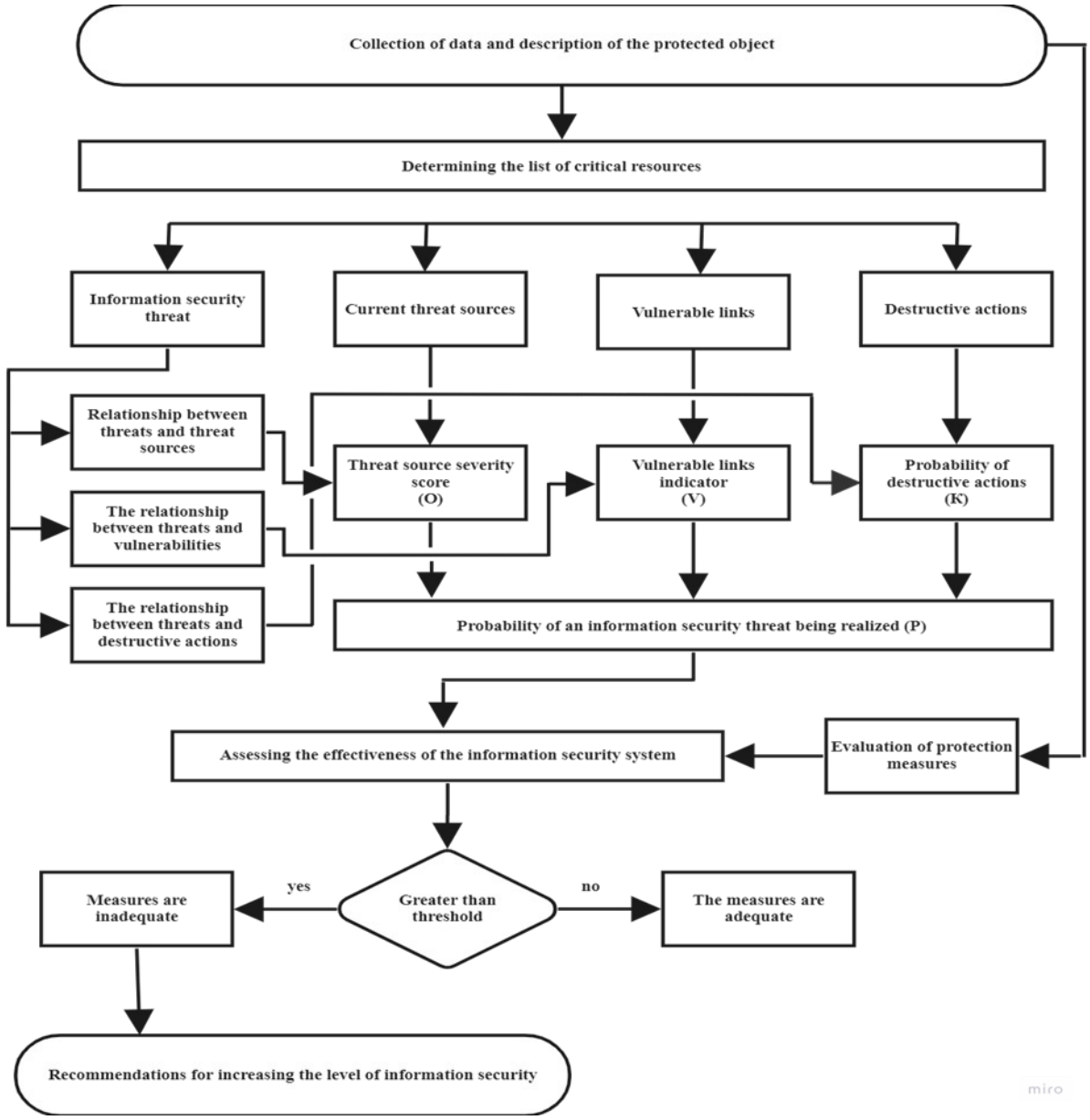

Figure 5: Algorithm for conducting an information security audit

This methodology, based on the input parameters and the results obtained, makes it possible to make an informed decision on the modernization of the security system and the implementation of a set of organizational and technical security measures. The proposed methodology can be used not only for information systems but can also be easily adapted to other objects, such as grid systems, virtual infrastructures, and cloud computing.

4. Determining the effectiveness of a security audit

To assess the effectiveness, it is necessary to compare the most important factors of the developed method with the benchmark factors. These factors should be significant enough to impact the quality and effectiveness of the IS audit significantly. Such factors will be: objectivity of the results of the IS audit, experience and qualifications of specialists conducting the IS audit, cost of the IS audit, adaptation of the method to the specifics of the organization, and simplicity of the technique in understanding and application. A benchmark is an "ideal" method of ensuring and conducting an information security audit. The comparison is made by mathematical calculations using the additive process.

The additive method of calculating the IS audit method weight consists of a weighted sum of private criteria. The weighting factor of the IS audit method is calculated within the framework of the accepted additive model of the calculation method. The efficiency coefficient of the IS audit method is as follows:

$$W(S)=\sum_{f=1}^{N} a_f s_f(S), \tag{19}$$

where S_1 is a reference IS audit method; S_2 developed IS audit method; $W(S)$ is the effectiveness coefficient (weight) of the IS audit method. The f index plays the role of the factor number; N is the number of factors; a_f is a coefficient characterizing the contribution of each of the factors $s_f(S)$ to the weight of the audit method's effectiveness: $\sum_{f=1}^{N} a_f=1; 0\le a_f\le 1$; $s_f(S)$ are partial indicators (coefficients) of a specific factor characterizing the quality and effectiveness of the IS audit method $0\le s_f(S)\le 1$. Coefficients a_f and partial indicators $s_f(S)$ are determined by experts (Table 2).

Table 2

Values of coefficients and partial indicators for the final values of the effectiveness of the reference and developed IS audit methods

#	Factors affecting method efficiency	Degree of significance coefficient	Partial indicator reference method	Partial indicator of the developed method
1	Objectivity of IS audit results	0.35	1	0.8
2	Experience and qualifications of specialists conducting an IS audit	0.25	1	0.7
3	Cost of conducting an IS audit	0.15	1	0.9
4	Adapting the method to the specifics of the organization	0.15	1	0.9
5	Simplicity of the method in understanding and conducting an IS audit	0.10	1	0.9
	Final method efficiency ratio		1	0.82

The formula for the final values of the effectiveness of the reference method of IS audit S_1 is as follows:

$$W(S_1)=0.35\cdot s_1(S_1)+0.25\cdot s_2(S_1)+0.15\cdot s_3(S_1)+0.15\cdot s_4(S_1)+0.10\cdot s_5(S_1),$$
$$W(S_1)=0.35\cdot 1+0.25\cdot 1+0.15\cdot 1+0.15\cdot 1+0.10\cdot 1=1. \tag{20}$$

The formula for the final values of the effectiveness of the developed IS audit method S_2 is as follows:

$$W(S_2)=0.35\cdot s_1(S_2)+0.25\cdot s_2(S_2)+0.15\cdot s_3(S_2)+0.15\cdot s_4(S_2)+0.10\cdot s_5(S_2),$$
$$W(S_1)=0.35\cdot 0.80+0.25\cdot 0.70+0.15\cdot 0.90+0.15\cdot 0.90+0.10\cdot 0.90=1. \tag{21}$$

Based on the calculations, we can conclude that the effectiveness of the developed IS audit method is $W(S_2)=0.82$. This is a relatively high indicator of the effectiveness and reliability of the method.

The advantages of the developed method are a high efficiency ratio, a combination of quantitative and qualitative assessments, consideration of the organization's characteristics, ease of understanding and use, the ability to assess the level of IS without involving external specialists and high costs, application at all stages of the organization's existence and consideration of the

ratio of losses, threats, level of IS, attitude to risks and costs of ensuring IS [3, 8–11, 15–17, 19, 23, 25]. The disadvantages of the method are the lack of an estimate of losses and audit costs in monetary terms and the need for highly qualified audit staff.

5. Characterization of the security model based on secondary agents

The enterprise application model is a structured approach to developing software to address enterprise management and IT tasks, including functions such as software distribution, security, logging, and network maintenance. It integrates various functions into a single product, providing centralized management across devices and operating systems. An important aspect is improving security with agents that monitor and respond to events, adapting to different platforms. However, security is often secondary, creating opportunities to strengthen audit logs in a security context. Enterprise software packages integrate system administration, which allows you to solve various tasks of managing the company's information environment. However, these programs have a disadvantage in the security field, as security audit is only a secondary component, which opens up opportunities to improve the effectiveness of audit logs [15–17, 20, 22, 24, 25].

The agent-based security model uses software modules to monitor, analyze, and respond to events in an information system. This allows automating monitoring and security processes, particularly through control over security policies and threat detection. Security agents monitor audit logs, recording violations of technical guidelines, adapting to different platforms and operating systems. Still, their work requires specialists to create new rules for each security policy, complicating management [10–13, 18, 19]. The limitations of the agent-based security model include high resource consumption, agent compatibility with system elements, deployment complexity, and the need for regular updates to respond to new threats. They can increase the load on the system, reducing performance, especially if there are many policies, which complicates management and requires significant effort to configure and maintain.

Agents only select individual lines in audit logs, which limits the ability to detect threats proactively. The isolation of agents on different platforms can reduce the effectiveness of detecting threats associated with activities at various system levels. In addition, expensive enterprise packages primarily available to large corporations put SMBs at a disadvantage, as existing tools cannot perform detailed log analysis to detect serious security breaches. Agent-based security models have limitations regarding the efficiency of searching and analyzing logs, which require significant resources. It is optimal to use specialized servers to process logs, which will reduce overhead costs, increase the effectiveness of security policies, and ensure the transition to a proactive approach to security management [15–17, 23–25].

6. Security model based on the primary agent

The primary agent-based security model involves using agents to actively monitor user activity and detect security breaches through analyzing audit logs, which allows for proactive threat detection instead of a reactive response. This approach helps to prevent security breaches by focusing on user activity, access to resources, and use of privileges, which increases the efficiency of detecting and responding to threats to ensure information security. A prototype security model based on a primary agent using proactive auditing was developed to effectively monitor user activities, particularly to detect security breaches through audit logs, as opposed to the traditional reactive approach [5, 19, 20].

The overall concept of a proactive audit log differs from the agent approach used in a secondary agent-based security model designed to reduce the processing overhead of application servers or workstations. Compared to the traditional approach, where the agent is used on application servers or workstations and adds processing to the normal activities of the computer, the new approach proposes to use a dedicated log server that performs audit log analysis [16, 17, 25]. This server will

combine and duplicate all platform-independent audit logs created by computers in the company (Fig. 6).

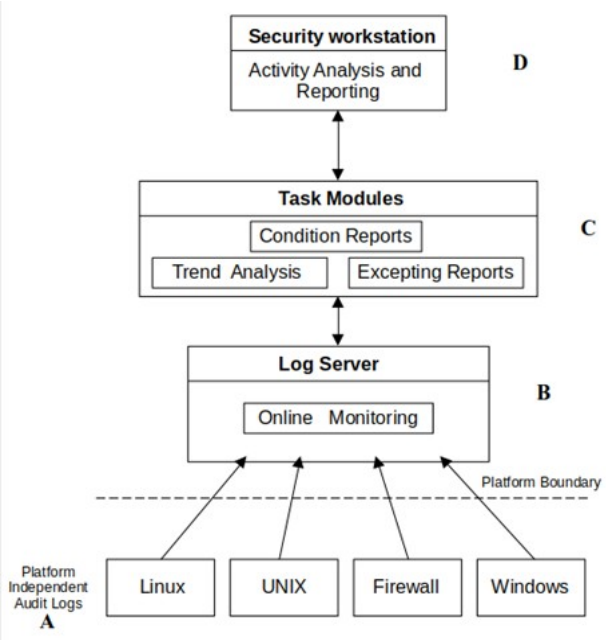

Figure 6: General model of a proactive security audit log

Proactive analysis of the audit log on the log server is carried out using modules that include exception analysis, trending, and security status reporting, which allows you to effectively detect security breaches and inform information security professionals about anomalies [15, 24, 25]. The modules are part of the overall proactive audit model, which consists of four components: a platform for data logging and duplication, a central server for storage and monitoring, task modules for real-time analysis, and a security workstation with a graphical interface for interacting with audit logs. The data logging platform provides segregated storage for analysis, preventing impact on system performance. The log server acts as a central data repository and online monitoring tool, generating reports whenever a breach is detected. Task modules perform real-time analysis, including status, exception, and trend reports that identify security anomalies over long periods, but are resource-intensive. The security workstation uses an interface to interact with logs and automatically displays breach notifications. The model also includes an analysis tool using a powerful query language for regular and one-time analysis of security logs. The goal is to create an "intelligent system" that not only interprets events but also alerts personnel to potential security breaches, responding to events that may occur in the future.

7. Strengthening security in the overall proactive audit log model

Strengthening the security of the general proactive audit log model involves measures to improve the protection of the information environment, including maintaining access control, enhancing security policies, monitoring threats, raising staff awareness, and regular auditing to identify weaknesses. The model consolidates logs from different platforms (UNIX, Linux, etc.) on a central log server, providing online monitoring and reporting functions for exceptions and system status.

Integrating audit logs from different operating systems is challenging due to the lack of common standards, which requires data cleansing to remove unnecessary information before saving it. In addition, detecting security breaches involves the integration of intelligent alerts that adapt to the severity of the incident, as well as specialized tools to implement high-level security policies in the corporate environment.

Recognition of hacker attacks is possible by identifying typical signs that appear in logs, which allows for the development of scripts to detect security breaches by comparing data with theoretical attack patterns [4, 15–17, 23–25]. The system should be able to determine the most effective notification methods, considering the availability of security personnel. At the same time, centralized log processing on a log server creates an additional load on the network due to increased traffic associated with data duplication. The overall model includes highly developed analysis tools and integration with other systems to identify security breach trends across different platforms. This allows for the timely detection of potential threats and notification of the relevant security authorities.

Conclusion

The effectiveness of information security audit control of information systems using audit logs largely depends on the system's ability to detect and respond to potential threats in real time. To achieve high efficiency, collecting and processing audit data correctly and applying modern risk assessment methods that allow you to monitor the system's state and adapt protection by changing threats is crucial. Using fuzzy Petri net models to model audit and security control enables you to determine the effectiveness of measures and the interaction between different stages of the audit, which increases the ability to predict new threats and respond quickly to them.

The audit methodology, which includes a quantitative assessment of the security system's effectiveness, provides an opportunity to make informed decisions on improving security measures and adapting them to new conditions. This universal approach can be adapted to different information systems, including grid systems, virtual infrastructures, and cloud computing, expanding these methods' scope.

An active audit system that uses fuzzy logic to make real-time decisions allows you to quickly neutralize threats and identify new attack patterns through reverse tracking analysis. This increases the reliability of protection and enables the generation of new security policies automatically implemented in the system without user intervention. Prospects for further research in this area will contribute to creating software that can effectively respond to unknown threats by automatically creating new attack patterns and corresponding security policies.

Declaration on Generative AI

While preparing this work, the authors used the AI programs Grammarly Pro to correct text grammar and Strike Plagiarism to search for possible plagiarism. After using this tool, the authors reviewed and edited the content as needed and took full responsibility for the publication's content.

References

[1] A. Ziro, et al., Research of the information security audit system in organizations, in: IEEE Int. Conf. on Smart Information Systems and Technologies (SIST), 2023, 440–444. doi:10.1109/sist58284.2023.10223557

[2] Y. Xu, et al., Review on cyber vulnerabilities of communication protocols in industrial control systems, in: IEEE Conf. on Energy Internet and Energy System Integration (EI2), 2017, 1–6. doi:10.1109/ei2.2017.8245509

[3] A. Mahfuth, et al., A systematic literature review: Information security culture, in: Int. Conf. on Research and Innovation in Information Systems (ICRIIS), 2017, 1–6. doi:10.1109/icriis.2017.8002442

[4] A. Edegbeme-Beláz, A. Kerti, A new approach to information security auditing in public administration, Hadmérnök, 17(3) (2022) 109–131. doi:10.32567/hm.2022.3.8

[5] D. A. Appelbaum, A. Kogan, M. A. Vasarhelyi. Analytical procedures in external auditing: A comprehensive literature survey and framework for external audit analytics, J. Account. Lit. 40(1) (2018) 83–101. doi:10.1016/j.acclit.2018.01.001

[6] S. D. Gantz, IT audit fundamentals. The basics of IT audit, 2014, 1–19. doi:10.1016/b978-0-12-417159-6.00001-8
[7] C. Vroom, R. Solms, Information security: Auditing the behaviour of the employee, in: Security and Privacy in the Age of Uncertainty, 2003, 401–404. doi:10.1007/978-0-387-35691-4_35
[8] T. Herath, H. Herath, Information security auditing—A decision model for performance evaluation, SSRN Electr. J., 2010. doi:10.2139/ssrn.1534192
[9] O. Kryvoruchko, et al., Analysis of technical indicators of efficiency and quality of intelligent systems, J. Theor. Appl. Inf. Technol. 101(24) (2023) 127–139.
[10] Z. Wang, S. Wang, L. Wang, Research on information security audit base on semantic web ontology and improve vector space model, Int. J. Secur. Its App. 10(12) (2016) 141–152. doi:10.14257/ijsia.2016.10.12.12
[11] A. Anon, Information system security audit, Manag. Account. J. 56(9) (2021).
[12] M. Gulzira, et al., The audit method of enterprise's Information security, in: 6th Int. Conf. on Engineering & MIS (ICEMIS), 2020, 1–5. ACM. doi:10.1145/3410352.3410761
[13] L. Jin, et al., Research on information security testing technology of relay protection equipment, in: 2nd Int. Conf. on Testing Technology and Automation Engineering (TTAE), 2022, 11. SPIE. doi:10.1117/12.2660304
[14] Y. Kostiuk, et al., Integrated protection strategies and adaptive resource distribution for secure video streaming over a Bluetooth network, in: Cybersecurity Providing in Information and Telecommunication Systems II, vol. 3826, 2024, 129–138.
[15] H. Janssen, Decentralized data processing: Personal data stores and the GDPR, Int. Data Priv. Law, 10(4) (2020) 356–384. doi:10.1093/idpl/ipaa016
[16] Z. Zeng, et al., Watson: Abstracting behaviors from audit logs via aggregation of contextual semantics, in: 28th Annual Network and Distributed System Security Symposium, NDSS, 2021.
[17] S. Majumdar, et al., Learning probabilistic dependencies among events for proactive security auditing in clouds, J. Comput. Secur. 27(2) (2018) 165–202. doi:10.3233/jcs-181137
[18] N. U. Ibne Hossain, et al., Modeling and assessing cyber resilience of smart grid using Bayesian network-based approach: a system of systems problem, J. Comput. Des. Eng. 7(3) (2020) 352–366. doi:10.1093/jcde/qwaa029
[19] O. Kryvoruchko, et al., Implementation of procedure for the identification of dynamic systems based on neural networks: Software engineering and cybersecurity, in: Int. Conf. SECS-2022, 2023, pp. 46–58.
[20] T. H. Morris, P. Shengyi, U. Adhikari, Cyber security recommendations for wide area monitoring, protection, and control systems, in: 2012 IEEE Power and Energy Society General Meeting, 2012, 1–6. doi:10.1109/pesgm.2012.6345127
[21] C. Lakos, Object oriented modelling with object Petri nets, in: Lecture Notes in Computer Science, 2001, 1–37. doi:10.1007/3-540-45397-0_1
[22] Y. Kostiuk, et al., Research of methods of control and management of the quality of butter on the basis of the neural network, in: Int. Conf. on Smart Information Systems and Technologies (SIST), 2022, 1–6. doi:10.1109/sist54437.2022.9945764
[23] Y. Kostiuk, et al., Information protection and data exchange security in wireless mobile networks with authentication and key exchange protocols. Cybersecur.: Edu. Sci. Technol. 1(25) (2024) 229-252.
[24] C. Regueiro, et al., A blockchain-based audit trail mechanism: Design and implementation. Algorithms 14(12) (2021) 341. doi:10.3390/a14120341
[25] F. Yang, et al., A flexible approach for cyber threat hunting based on kernel audit records, Cybersecur. 5(1) (2022). doi:10.1186/s42400-022-00111-2