Date of publication DEC-31, 2024, date of current version AUG-11, 2024.
www.computingonline.net / computing@computingonline.net

Print ISSN 1727-6209
Online ISSN 2312-5381
DOI 10.47839/ijc.23.4.3770

Methodology for Determining Means of Monitoring Information Security by the Method of Expert Assessment

SVITLANA LEHOMINOVA, MYKHAILO ZAPOROZHCHENKO, YURII SHCHAVINSKY, TETIANA MUZHANOVA, VITALII TYSHCHENKO, MATVII YUSHCHENKO

State University of Information and Communication Technologies, Kyiv, Ukraine

Corresponding author: Yurii Shchavinsky (e-mail: yushchavinsky@ukr.net).

ABSTRACT The article examines and analyzes the numerous advantages of using information technologies to ensure the information security of organizations in connection with the wide spread of the number of modern methods of cyber attacks. It is established that effective cyber protection requires an information security management system with a set of modern event monitoring tools depending on the specifics of each organization. To select an appropriate system and evaluate the effectiveness of its tools, the method of expert evaluation is used in the work. In order to improve the determination of the weight coefficient of each tool of the system, a composite indicator is proposed, based on the sum of the products of individual indicators of the system tools and their priority coefficients. The features of the modern widely used solutions considered in the study confirmed the feasibility of the proposed methodology for determining effective tools of the information security monitoring system. The resulting data allows us to help organizations make an evidence-based decision about the optimal composition of the information security monitoring system.

KEYWORDS information security; information security monitoring; cyber security; event management.

I. INTRODUCTION

GIVEN the current state of the information technology sector, it becomes necessary for the effective development of an organization to develop and ensure the functioning of the secure information environment based on the use of advanced automated technical solutions and modern information security practices.

In the process of developing and implementing organizational measures and integrated information security systems, inadequate attention is often paid to monitoring the security of network equipment, e-mail, messengers, and personnel activity. This leads to untimely receipt of information about potential threats, vulnerabilities, incidents, and other events occurring in the corporate information system. As a result, organizations suffer serious financial, reputational, and other losses due to a breach of confidentiality of corporate information.

In this regard, the corporate information security policy should be carefully structured to take into account the organization's needs to monitor both external and internal processes, protect confidential information and infrastructure, and, importantly, the role of personnel as a potential source of internal threats to the organization. The security policy should establish requirements for implementation of automated tools that help monitor external and internal processes in the interests of ensuring the organization's information security.

The modern information security market offers a large number of solutions for monitoring, detecting and responding to information threats, many of which demonstrate similar functionality and affordability. This situation complicates the process of choosing the optimal solution, taking into account the specifics, needs and capabilities of the organization, while the implementation of the most appropriate solution directly affects the organization's ability to effectively respond to information threats and protect confidential data.

The scientific task in this context is to develop a methodology for an objective and rational choice of an information security monitoring solution depending on the specific needs and characteristics of the organization.

II. LITERATURE REVIEW

The assessment of cybersecurity is crucial to ensure that security measures in organizational infrastructures, systems, and applications meet necessary requirements. Over the years of cybersecurity development, a sufficient number of assessment methodologies have been proposed in scientific

publications. Special attention has been paid to the aspect of the quality of their applications or suitability for use. However, as the analysis of scientific literature including journals, books, and databases of well-known publishers, namely Scopus, Web of Science (WoS), ACM Digital Library, Elsevier, Emerald, IEEE Xplore, Springer, and Wiley, in which the issues of information security, communication systems, computer science, etc. have been highlighted, shows that there are practically no evaluations of the effectiveness of these methods [1-4].

In the works of researchers [5-9], concerns were articulated regarding the lack of comprehensive literature analysis on the security system assessment compared to the risk and threat assessment. Researchers argued that Security Control assessment should be empowered in accordance with the international standards [10] to ensure that security implementation is effective and provides the expected protection [11-13].

A review of recent methodologies and tools for measuring and assessing cybersecurity based on best practices in network security measurement and modern corporate data transmission network protection was presented in paper [14]. The analysis was based on the study of methods for measuring and assessing information security at the physical-technical level, penetration testing, and identification of weaknesses in the cybersecurity system adhered to, as well as policies used in modern enterprises. Risks dependence on technologies and their impact on the economic market index of enterprises, reputation, and the security of individuals and enterprises were identified, prompting experts and decision-makers to consider information security and develop new methods for measuring and assessing the level of information and data protection in enterprises and the confidentiality of individuals.

In study [15], the need for validation of information security assessment scales was identified. In the analysis, the author pointed out that in most studies, scientists had provided somewhat limited evidence for the validation of scales. In particular, critical problems are the lack of evidence for discriminant and criterion validity.

Paper [16] examined an expert system providing an assessment of the state of information security in government agencies and organizations of various ownership forms. The proposed expert system allows evaluating compliance with both organizational and technical requirements for ensuring information protection, as well as the level of compliance with the requirements of the information security system as a whole. The expert assessment method is used as the basic method for evaluating the state of information security. The developed expert system significantly reduces routine operations during information security audits. The assessment results were presented quite clearly enabling the governmental authorities in agencies and organizations to make informed decisions regarding further improvement of the information security system.

At a recent time, researchers have been paying significant attention to the application of artificial intelligence (AI) in information security. In work [17], a comprehensive review of vulnerability assessment methods with a particular focus on AI applications was conducted. This review examined 20 approaches based on artificial intelligence, including machine learning, automated planning, and expert systems. In addition, the authors in their studies [18-19] identified directions for further research, highlighting gaps in knowledge regarding the evaluation of the use of security methods and presenting valuable guidelines for future research.

Currently, maturity models play a central role in the concept of Information Security Management Systems (ISMS) providing a framework for measuring information security. These models also require research and evaluation. A novel idea in the application of such models lies in the systematic assessment of process maturity related to the security within an organization. This allows decision-makers to gain an overview of the implementation status of relevant processes for identifying critical points. Research [20] found that some industries, such as the German automotive sector, even established security maturity levels as a de facto standard for measuring information security. However, researchers in their works [21-25] noted that the quality of the security maturity level assessment was still insufficiently researched, and security managers could not accurately assess the maturity level of security controls. In study [20], where security experts evaluated a subset of ISO/IEC 27002 security controls for a hypothetical scenario using COBIT maturity levels, it was found that many security experts struggled with this task.

The analysis of scientific publications indicates that there is a necessity for researchers to determine suitable information security monitoring tools, search for and refine methods for assessing their effectiveness.

The purpose of the article is to study information security monitoring tools and develop a methodology for selecting and determining the most effective solutions from them using the method of expert assessments based on the specifics, needs and capabilities of a particular organization, as well as the peculiarities of ensuring information security in a particular corporate environment.

III. MATERIAL AND METHODS

A. GENERAL OVERVIEW OF INFORMATION SECURITY MANAGEMENT TOOLS

The term SIEM (Security Information and Event Management) first appeared in 2005 and was used to refer to a system designed to collect information from devices located on a corporate network. Today, SIEM systems are tools used to effectively manage information security in organizations, including systematic monitoring and analysis of events in real time and, as a result, detection of anomalies and potential threats to information security [26].

SIEM software collects log data and events from internal and external sources, which can include intrusion prevention and detection systems (IPS, IDS), server and computer logs, switches, routers, databases, antivirus platforms, remote access systems, data leakage (loss) prevention systems (DLP - Data Loss Prevention), user behavior monitoring systems, and file servers. This allows for a thorough analysis and provides a holistic view of the organization's information security status.

Modern recognized SIEM systems have a wide range of functionality, including data aggregation and correlation, event log management, alerts about existing and potential problems in the organization's infrastructure, visualization of information about system behavior through dashboards, ensuring compatibility with the infrastructure, and the ability to store events in the built-in data storage for further incident investigation [27-28].

While SIEM systems are mainly aimed to protect organization against technical processes, User Activity Monitoring (UAM) tools are used to prevent the influence of

the human factor on information security solutions. UAM systems are a set of software tools designed to systematically monitor and track user activity on various devices, in the network environment and other IT resources of the organization. The purpose of these tools is to help to identify and neutralize internal threats, whether they are accidental or intentional, and, accordingly, to ensure the availability and correctness of information confidentiality and security [29-30].

B. DESIGNATION OF THE USER ACTIVITY MONITORING MEANS

Tools can vary in approach and complexity, each serving distinct purposes tailored to the organization's goals. The main tools are shown in Figure 1 [31].

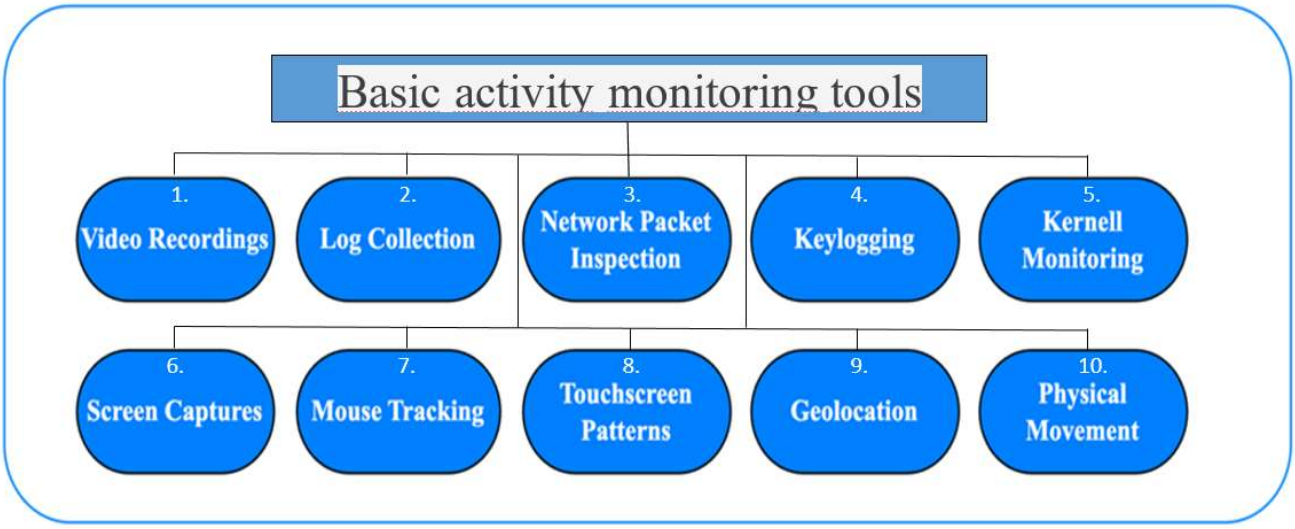

Figure 1. Basic tools for monitoring user activity [31]

1. Video recordings allow detecting suspicious behavior of employees, such as access to unauthorized areas, attempts to manipulate equipment or unauthorized copying of confidential documents, as well as understanding the nature of the threat and taking appropriate measures. Employees' awareness that their actions may be recorded often reduces the likelihood of internal threats, such as malicious or negligent attitudes toward their duties. Video recordings also provide reliable evidence for investigations of internal incidents.

2. Log collection provides a detailed record of what is happening on the network and systems, allowing auditing user actions, which is a key to identifying abnormal or dangerous actions that may be a sign of an internal threat. Thanks to integration with SIEM systems, logs allow information security specialists to automatically analyze suspicious activities or security policy violations, which allows them to respond quickly to internal threats. Analyzing logs after an incident can help to identify weaknesses in security systems, which makes it possible to improve policies and procedures to prevent similar threats in the future.

3. Network packet inspection allows analyzing data at different levels of the network stack, from the link layer (L2) to the application layer (L7), which makes it possible to identify anomalous patterns that may be missed by basic analysis. Using this tool, it is possible to control employees's network activity by detecting and blocking unacceptable actions, such as accessing prohibited websites, using unauthorized applications, or transmitting confidential information.

4. Keylogging allows recording every keystroke on the user's keyboard, which can provide valuable information for detecting malicious actions and attempts of unauthorized access to confidential data, including passwords, logins or other sensitive information. Keylogging makes it possible to monitor employees' compliance with security policies when working with confidential information, and provides a detailed record of all user actions on the keyboard, which can be used as evidence in the investigation of incidents related to internal threats. In the event of an incident, data from the keylogger can help to recreate the chronology of events, determine which actions led to the threat, and understand the motives of the potential attacker.

5. Kernell monitoring is a powerful tool for detecting and neutralizing internal threats, it allows us to control the lowest level of the operating system, where critical processes that ensure the operation of the entire system take place. Kernell monitoring makes it possible to detect abnormal or suspicious activities, such as attempts to change the system configuration, access to protected resources, or the execution of malicious programs.

6. Screen captures allows us to take screenshots of the user's screen in real time or at certain intervals, which makes it possible to observe what is happening on the device screen, and allows detecting attempts of malicious actions, such as access to confidential documents, use of unauthorized programs, or attempts to transfer data to third parties. Setting up screen captures to save images at key moments, such as entering passwords, opening confidential files, or during suspicious activity, helps to create a complete record of events that can be used during incident investigations.

7. Mouse tracking is more specific and less common method of detecting insider threats, but it can also affect an organization's security in certain contexts. Anomalies in mouse movements or interaction with the interface may indicate that the system is being used by someone other than the person who normally works on that computer, or that the user is acting under pressure. To create a more complete profile of the user activity and increase the accuracy of threat detection, this tool is used in conjunction with other monitoring tools such as keylogging or screen captures.

8. Touchscreen patterns allows us to track, analyze and store data on the user interaction with the touchscreen, including finger movements, gestures, clicks, and other actions performed on the touch surface. For example, each user has a unique style of interaction with the device (speed of movement, pressure, frequency of gestures). Detecting deviations from these familiar patterns can signal that the device is being used by an unauthorized person or that the user is acting under pressure.

9. Geolocation allows detecting the presence of a user or device in a place that does not correspond to the usual work area. For example, if an employee suddenly appears in another city or country, it can signal a possible data leak or device theft.

10. Physical Movement is an important element of the security system that makes it possible to record and analyze the physical movements of users or devices within the organization. It uses data from accelerometers, gyroscopes, motion sensors, cameras, or other devices to track movement. Physical movement data can be used to reconstruct events during an incident investigation. This allows you to recreate the user's route to determine whether they visited prohibited areas or were present in critical areas at the time of the suspicious activity.

Each method provides specific information and means of control, but the greatest effectiveness of activity monitoring can be seen with the integrated use of these specified tools.

All collected information should be reviewed within the framework of the organization's policies and user role, based on which a decision is made on the appropriateness of the activity. Modern user activity monitoring tools track the user activity in the background and in real time and alert security when suspicious activity occurs. This feature reduces the burden on an organization's IT teams to monitor the user activity in real time and reduces the likelihood that risks associated with the user activity will not be detected.

The functionality of SIEM and UAM solutions is most suitable for solving the problems of monitoring an organization's information security. It is advisable to consider SIEM as the main tool for monitoring processes and managing the security of information assets, and UAM as a key solution for monitoring external processes, user activity, mail, messengers, and social networks.

The current SIEM market is dominated by a few vendors with significant international influence, including IBM, Splunk, and HPE (Fig. 2).

Figure 2. Gartner Magic Quadrant for SIEM in 2022 [32]

Key players that are actively competing in this market include Alert Logic, Intel, LogRhythm, ManageEngine, Micro Focus, SolarWinds, and Trustwave.

This research aims to determine the most suitable Security Information and Event Management (SIEM) and User Activity Monitoring (UAM) tools through expert judgment. SIEM and UAM are critical components of cybersecurity infrastructure, aiding in threat detection, incident response, and compliance adherence. Given the plethora of available options, selecting the most effective tools requires informed decision-making based on expert insights.

C. CREATION OF AN EXPERT GROUP

The research adopts a qualitative approach to gather expert opinions and insights. Purposive sampling was employed to select experts with substantial experience and expertise in cybersecurity, specifically in SIEM and UAM implementation and management. Recognizing the multifaceted nature of SIEM functionality, a group of 7 experts was assembled to assess the relative importance of these attributes. The criteria for selecting experts included: professional experience; specialized skills and knowledge and their relevance; independence and objectivity; authority; and ethics and academic integrity. The high-quality composition of the group included: 1 Doctor of Science and 3 PhDs (all of whom had publications on the subject and experience in research and teaching cybersecurity courses) and 3 specialists from organizations with practical experience in operating SIEM.

Thus, the expert group consisted of cybersecurity professionals, academics, and industry practitioners with extensive experience in deploying and managing SIEM Expert opinions and judgments were collected through semi-structured interviews and expert surveys. Qualitative data from interviews and surveys was analyzed thematically to identify recurring patterns, criteria, and preferences in selecting SIEM and UAM tools.

Findings may be limited to the expertise and perspectives of the selected experts and may not be universally applicable.

IV. RESEARCH RESULTS

A. COMPARATIVE ANALYSIS OF SIEM SYSTEMS

The general purpose of SIEM systems for organizations is that, firstly, SIEM systems provide reports on incidents and events related to information security (successful and unsuccessful logins, malware activity and other possible malicious actions), and secondly, they send notifications about any activity that, according to the analysis, is performed in violation of predefined sets of rules and thus, indicates a potential security problem.

An analysis of the trends in the development of modern SIEM systems indicates that these solutions are primarily focused on meeting the basic needs of consumers. In particular, the current requirements for SIEM systems are to ensure full control and visibility of security events, the ability to effectively integrate with other information systems, reliability, ease of use, and competitiveness in terms of deployment costs.

It is important to note that when choosing the method of expert evaluation for analyzing SIEM systems and determining the indicators used for the assessment, no division has been made between the supplier and the consumer. Thus, the method itself is considered to be unified, but at the same time takes into account the strategy and the availability for cybersecurity market participants who may have an insufficient level of training. In addition, by applying the principle of weighting, each user of this method has the opportunity to adapt it depending on one's own capabilities and needs.

The main factor in assessing the effectiveness is that the indicators can also change their state and adapt to the applied mathematical apparatus by inversion. For example, changing the opposite states of mobility – stationarity, security – availability, complexity – simplicity, simplifies the objective determination of the advantages and disadvantages of each SIEM system. For example, a comparative table is provided, which contains the basic indicators for evaluation (Table 1).

Table 1. Comparison of modern SIEM systems by defined characteristics

№	Parameter	IBM QRadar	Splunk	HPE ArcSight
1	Architecture (On-premise, Cloud, SaaS)	On-prem Cloud SaaS	On-prem SaaS	On-prem Cloud
2	Complexity of implementation	Complicated	Complicated	Very complicated
3	Convenience of incident investigation functionality	More convenient	Convenient	Convenient
4	Details of data display	+	+	+
5	Automatic detection of event sources	+	+	+
6	Incident notification	SMTP	SMTP Месенджер	SMTP SMS
7	Ability to set or import information about assets	Security scanners CSV file API	-	ArcSight Asset Import Connector
8	Number of supported event sources	300+	2000+	300+
9	Ability to connect non-standard event sources	Parser development	Parser development	ArcSight Flex Connector
10	Availability of predefined correlation rules	+	+	+
11	Availability of predefined graphical panels (Dashboards)	+ QRadar Pulse	+	+
12	Availability of predefined reports	110+ Content Extension Pack	500+	80+
13	Availability of visualization panels and reports on compliance with standards (Compliance)	PCI DSS COBIT FISMA GLBA HIPAA NERC SOX	GDRP HIPAA FISMA PCI DSS	PCI DSS HIPAA SOX NERC FISMA
14	Ability to search by raw events	+	+	+
15	Work with filters	Filters by data fields Regex AQL	Filters by data fields SPL	Filters by data fields Full text search
16	Ability to build network interaction graphs	+	+	Between 3 hosts
17	Ability to generate reports in the form of documents (export formats)	PDF HTML RTF XML XLS	Raw PDF CSV XML JSON	PDF HTML XLS RTF CSV
18	Interactive work with graphical panels	+	+	+
19	Availability of HA (High Availability) and DR (Disaster Recovery)	HA DR	HA DR	HA
20	Ability to restore the database after failures	+	+	+
21	Aggregation of events by type	+	+	+
22	Normalization of events	+	+	+
23	Methods of collecting events from sources	Agent-based Agent-free	Agent-based Agent-free	Agent-based Agent-free
24	Supported event collection formats	Syslog TLS Syslog Log File SNMP, JDBC WinRPC OPSEC HTTP FTP SCP	Syslog Wineventlog Perfmon WMI OPSEC SNMP JDBC SDEE SQL	Syslog TLS Syslog Log File SNMP JDBC WinRPC OPSEC HTTP SCP
25	Ability to collect data on network traffic	SPAN Netflow J-flow sFlow	Netflow J-flow sFlow IPFIX HTTP XMPP	Netflow J-flow IPFIX
26	Behavioral analytics (UBA)	+	+	+
27	Integration with ITSM/CMDB	+	+	+
28	Connection of reputation databases	+	IBM X-force	ArcSight RepSM
29	Availability of API	REST API	REST API	WebAPI
30	Integration with vulnerability scanners	+	+	+

However, each of the groups of indicators can be expanded or reduced compared to the baseline values in accordance with the needs and requirements of a particular organization.

B. RESEARCH METHODOLOGY OF SIEM-SYSTEMS AND UEM-SYSTEMS USING THE METHOD OF EXPERT EVALUATION

To make a reasonable choice of the most appropriate SIEM system selected for the analysis, as well as to obtain

quantitative characteristics of their effectiveness, the method of expert evaluation is used. The evaluation algorithm is presented in Fig. 3.

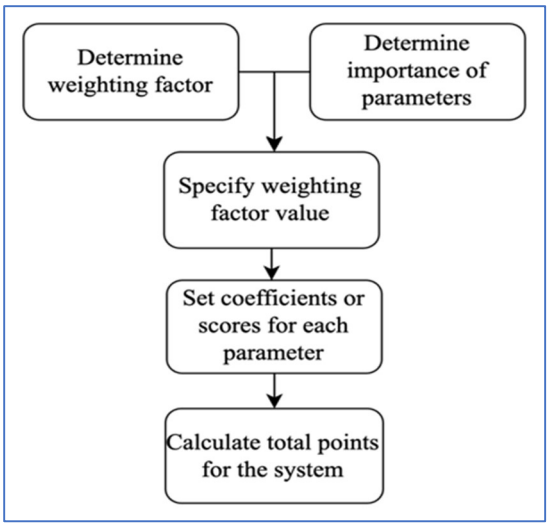

Figure 3. SIEM system evaluation algorithm

The first step is to determine the weighting factor for each of the indicators. In case of using both direct and inverse indicators, the value of each coefficient is in the range from 0 to 1. However, this approach complicates the calculations and reduces the level of technology disaggregation, which may be unacceptable.

For this purpose, a composite indicator based on the sum of individual indicators multiplied by coefficients that can take values in the range from 1 to 10, depending on the user's choice and ability to prioritize the properties of the indicators, can be used to simplify the evaluation using only direct indicators with the replacement of inverse indicators.

The next step is to determine the degree of importance of each parameter for building an information security monitoring system using SIEM, and each parameter is included in the appropriate group.

The division into groups can be made depending on the characteristics of the parameters, such as technical, economic, ergonomic, financial, and others. However, to simplify the process, it is sufficient to limit the grouping to suitability, preference, and optimality.

The third step is to specify the value of the weighting factor, which combines the first two steps. This coefficient can also have two directions. The first direction involves the selection of boundaries between groups depending on the value of the coefficient, and the second is based on the use of fixed values of the coefficients (Table 2).

Table 2. Example of determining the weighting factor

Points	Description	Points	Description
1-2	Does not meet the requirements	1	Does not meet the requirements
3	Belongs to the "suitability" group with restrictions		
4-7	Preferred compared to other options (the number of points determines the degree of preference)	5	Not the best option, but suitable for development (assigned to the "suitability" group)
8-9	Quasi-optimal	10	Meets the requirements and is the best option
10	Optimal		

The fourth step is to set coefficients or provide scores for each parameter separately for each system.

The fifth step involves calculating the total number of points for each SIEM system (S_1 – IBM QRadar, S_2 – Splunk, S_3 – HPE ArcSight) as the sum of the products of the coreesponding parameter score and its weighting factor according to the following formula:

$$S_k = \sum_{i=1}^{n} a_i \cdot M_i, \quad (1)$$

where S_k – total number of points for the k-th SIEM system, a_i – i-th parameter score, M_i – the weight factor of the system i-th parameter.

The last step is to select the best SIEM system among those compared using the following formula:

$$S = \frac{S_k}{A \cdot M_{max}}, \quad (2)$$

where A – the maximum number of points, M_{max} – maximum weight factor.

SIEM systems play a pivotal role in modern cybersecurity frameworks, enabling organizations to aggregate, correlate, and analyze security event data from disparate sources. The efficacy of SIEM deployments is contingent upon numerous parameters and characteristics, ranging from scalability and flexibility to detection capabilities and user interface intuitiveness. Recognizing the multifaceted nature of SIEM functionality, a panel of experts was convened to assess the relative importance of these attributes.

The expert panel comprised cybersecurity professionals, academics, and industry practitioners with extensive experience in SIEM deployment and management. A structured survey instrument was developed, encompassing a comprehensive set of parameters and characteristics relevant to SIEM systems. Panelists were tasked with rating each attribute on a predefined scale, reflecting its importance in the context of SIEM implementation. Statistical analyses, including mean scores and standard deviations, were employed to synthesize the expert responses and derive consensus rankings.

Using formula 1 ($M_{max}=10$), the SIEM systems IBM QRadar, Splunk, and HPE ArcSight were compared (Table 3).

Table 3. Comparison of modern SIEM systems based on the importance of parameters

№	Parameter	IBM QRadar	Splunk	HPE ArcSight	M_i
1	Architecture (On-premise, Cloud, SaaS)	10	7	7	7
2	Complexity of implementation	8	7	5	10
3	Convenience of incident investigation functionality	9	8	8	10
4	Details of data display	10	10	10	9

№	Parameter	IBM QRadar	Splunk	HPE ArcSight	M_i
5	Automatic detection of event sources	10	10	10	7
6	Incident notification	8	10	10	8
7	Ability to set or import information about assets	10	0	9	8
8	Number of supported event sources	7	10	7	10
9	Ability to connect non-standard event sources	8	8	9	8
10	Availability of predefined correlation rules	10	10	10	10
11	Availability of predefined graphical panels (Dashboards)	10	9	9	10
12	Availability of predefined reports	9	10	8	8
13	Availability of visualization panels and reports on compliance with standards (Compliance)	10	7	9	10
14	Ability to search by raw events	10	10	10	9
15	Work with filters	10	7	5	10
16	Ability to build network interaction graphs	10	10	6	10
17	Ability to generate reports in the form of documents (export formats)	9	9	9	6
18	Interactive work with graphical panels	10	10	10	9
19	Availability of HA (High Availability) and DR (Disaster Recovery)	10	10	7	9
20	Ability to restore the database after failures	10	10	10	10
21	Aggregation of events by type	8	7	7	7
22	Normalization of events	10	10	10	10
23	Methods of collecting events from sources	10	10	10	7
24	Supported event collection formats	10	8	9	10
25	Ability to collect data on network traffic	8	10	7	10
26	Behavioral analytics (UBA)	10	10	10	9
27	Integration with ITSM/CMDB	10	10	10	7
28	Connection of reputation databases	10	7	9	10
29	Availability of API	9	9	8	8
30	Integration with vulnerability scanners	10	10	10	10
Maximum number of points, taking into account the weighting factors		2660			
Total number of points for systems		2512	2338	2277	–

Note: M_i is the weighting factor of the parameter.

The results of the analysis of the choice of SIEM technology from the compared ones should be regarded as the results summarized in Fig 4.

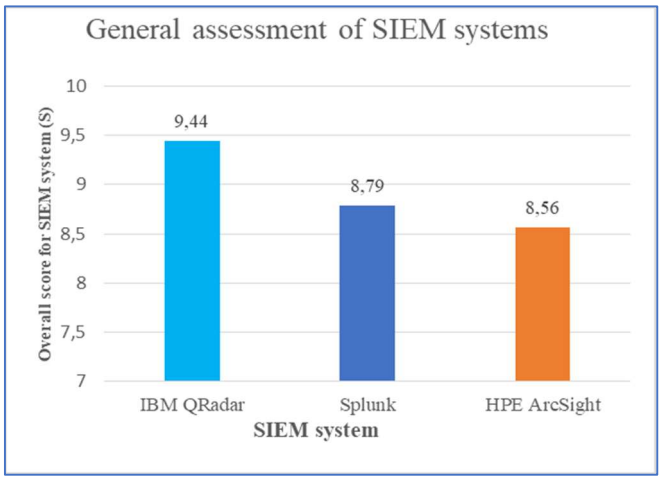

Figure 4. The results of the analysis of selecting SIEM technology

The above example, which does not claim to be a general assessment in its entirety, but is based on the limitations introduced, and is also more abstract due to the use of a simplified methodology, allows us to draw the following conclusion: taking into account the selected parameters, among modern SIEM systems, IBM QRadar has an advantage with the received 9.44 points and is recommended for implementation as the most acceptable. Splunk is close to it in terms of key indicators and overall score.

An analysis of modern methods used by attackers to conduct cyberattacks using social engineering techniques has revealed three key ways to implement threats: email, social networks, and instant messengers.

These methods require close monitoring due to their vulnerability to being used by insiders to steal confidential data. To solve these problems, it is recommended to implement the user activity monitoring systems, the most widely used of which are the following: Teramind UAM; Ekran System Enterprise Edition; Mirobase.

An analysis of trends in the development of modern user activity monitoring systems shows that consumers focus on a number of key requirements, among which the main ones are: the importance of recording work sessions in video format, the ability to monitor email, messengers and social networks, system reliability, accessibility, ease of use, the ability to generate analytical reports and integration with SIEM.

For a comparative analysis of the user activity monitoring systems, we suggest using the parameters (characteristics) presented in Table 4.

Table 4. Comparison of modern UAM systems

№	Parameter	Ekran System	Mirobase	Teramind
1	Completeness of OS support (Windows, Linux, MacOS)	Windows Linux MacOS	Windows Linux	Windows MacOS
2	Architecture (On-premise, Cloud, SaaS)	On-prem Cloud	On-prem	On-prem Cloud SaaS
3	Providing recording of the working session in video format	+	+	+
4	Ability to record sessions in offline mode	+	-	-
5	Linking the event log to each screenshot	+	+	+
6	Viewing sessions in Live mode	+	+	+

№	Parameter	Ekran System	Mirobase	Teramind
7	Flexible configuration of monitoring parameters for each machine	Flexible	Standard	Flexible
8	Application and web page (URL) monitoring	+	+	+
9	Clipboard monitoring (copy/paste)	+	+	+
10	Monitor USB device connections	+	+	+
11	Mail monitoring	-	+	+
12	Monitoring of instant messengers	-	+	+
13	Social media monitoring	-	-	+
14	Monitoring console commands and their parameters	-	-	+
15	Remote installation/removal/update of agents	+	-	+
16	Agent protection against modifications	+	-	-
17	Monitoring filtering and keyword search in sessions	+	+	+
18	Availability of the OCR (Optical Character Recognition) module	-	-	+
19	System reliability	+	-	+
20	System availability	Expensive	Cheap	Average
21	Simplicity of use	Complicated	Complicated	Very complicated
22	Ability to generate analytical reports	+	+	+
23	Integration with SIEM	+	-	+
24	Notification of the administrator about violations of behavioral rules	+	+	+

Applying a similar expert evaluation approach to that used to determine the optimal SIEM system, the following quantitative results are obtained for comparing the UAM systems Ekran System, Mirobase, and Teramind (Table 5).

Table 5. Comparison of modern UAM systems taking into account the importance of parameters

№	Parameter	Ekran System	Mirobase	Teramind	M
1	Completeness of OS support (Windows, Linux, MacOS)	10	6	6	10
2	Architecture (On-premise, Cloud, SaaS)	7	5	10	8
3	Providing recording of the working session in video format	10	8	10	10
4	Ability to record sessions in offline mode	10	0	0	6
5	Linking the event log to each screenshot	10	8	10	8
6	Viewing sessions in Live mode	10	10	10	9
7	Flexible configuration of monitoring parameters for each machine	10	6	10	9
8	Application and web page (URL) monitoring	10	10	10	10
9	Clipboard monitoring (copy/paste)	10	10	10	8
10	Monitor USB device connections	9	8	9	6
11	Mail monitoring	0	8	10	10
12	Monitoring of instant messengers	0	9	10	10
13	Social media monitoring	0	0	8	10
14	Monitoring console commands and their parameters	0	0	8	7
15	Remote installation/removal/update of agents	10	0	8	5
16	Agent protection against modifications	10	0	0	8
17	Monitoring filtering and keyword search in sessions	10	7	10	9
18	Availability of the OCR (Optical Character Recognition) module	0	0	10	7
19	System reliability	8	5	9	10
20	System availability	6	10	9	10
21	Simplicity of use	8	6	10	10
22	Ability to generate analytical reports	9	7	9	9
23	Integration with SIEM	10	0	10	10
24	Notification of the administrator about violations of behavioral rules	8	7	10	8
Maximum number of points, taking into account the weighting factors		2070			
Total number of points for systems		1495	1178	1811	–

Using formulas 1 and 2, values are obtained to evaluate each of the compared UAM systems (Fig. 5).

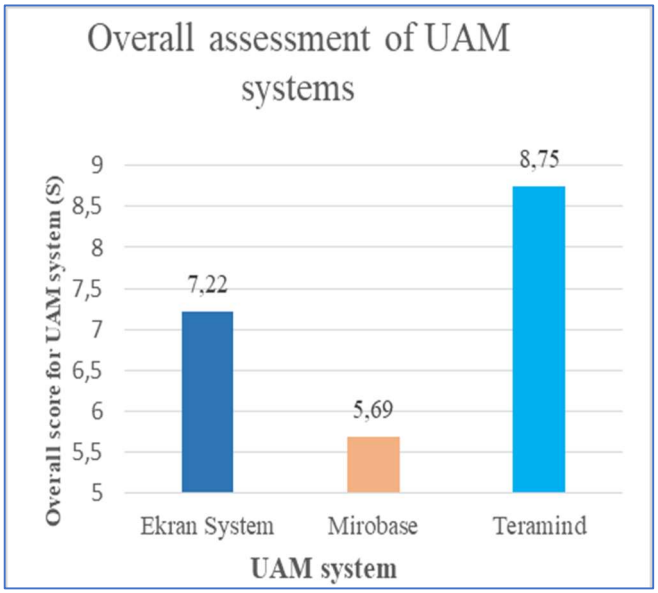

Figure 5. The results of the analysis of selecting UAM systems

Thus, the best performance is shown by the UAM Teramind system, which has scored 8.75 points and is recommended for implementation as the most acceptable.

Based on the obtained values of the evaluation of management and monitoring solutions, the following general scheme for monitoring the organization's information security based on the IBM QRadar SIEM system and the Teramind user activity monitoring system is proposed (Fig. 6).

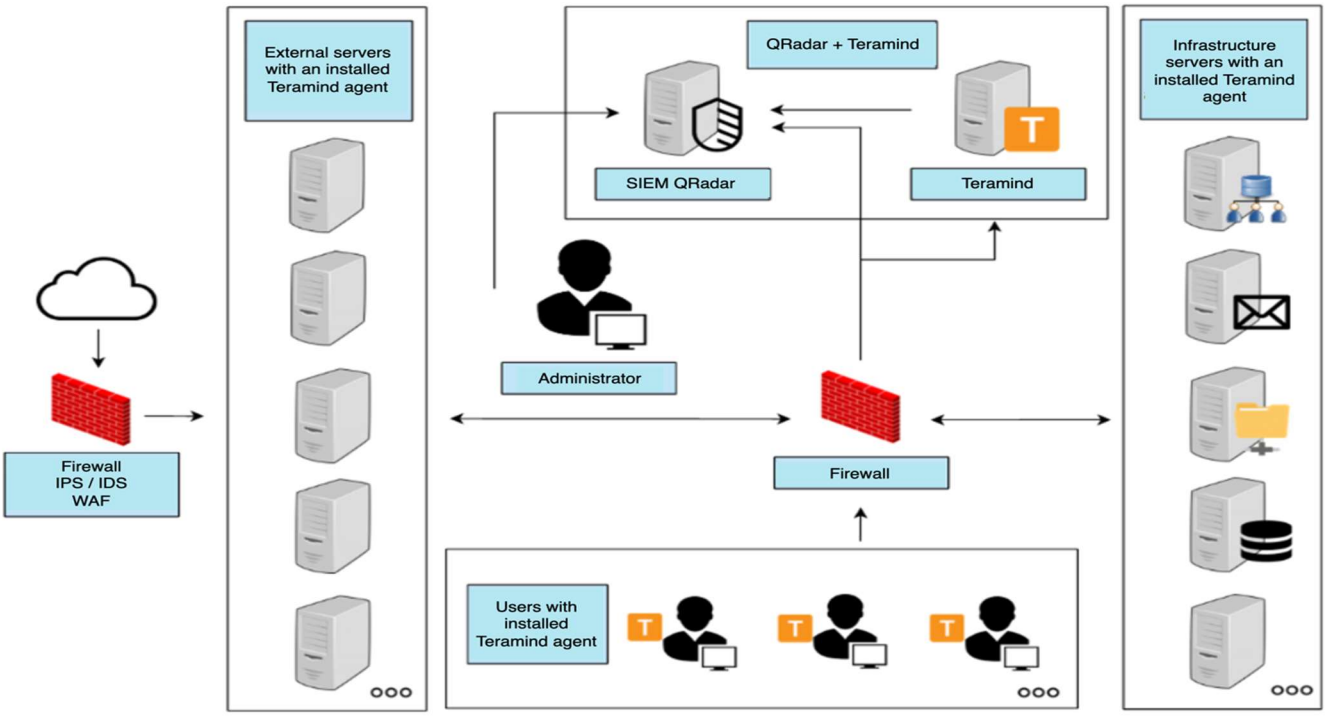

Figure 6. General scheme for monitoring external and internal processes of an enterprise based on IBM QRadar and Teramind

V. CONCLUSIONS AND PROSPECTS FOR FURTHER RESEARCH

The analysis of scientific literature conducted in this work has revealed the need for developing a methodology for selecting the optimal combination of software solutions and tools for effective monitoring of an organization's information security. It is found that for effective cybersecurity, considering the specifics of each organization, a security management system with a set of modern event monitoring tools is required. To create such a system, it is necessary to select an effective combination of tools that can ensure reliable cybersecurity for the organization.

The proposed methodology for using the expert method in evaluating tools, along with the refined weighting coefficient and the composite index based on the sum of the products of individual tool indicators and their priority coefficients, allows organizations to choose the most appropriate tools and make an informed decision regarding the optimal composition of the information security monitoring system, taking into account the specifics of each organization.

The effectiveness of this methodology is confirmed by comparing major SIEM and UAM systems. The overall evaluation for each SIEM system under study is obtained by assessing 30 specified parameters using a sample of three representatives (IBM QRadar, Splunk, HPE ArcSight). Similarly, an overall evaluation for UAM systems is obtained based on 24 specified parameters of modern UAM solutions using a sample of three representatives, namely Ekran System, Mirobase, Teramind. Based on the evaluation of several management and monitoring solutions, a general scheme for monitoring an organization's information security is developed using the SIEM system IBM QRadar and the UAM system Teramind. The implementation of this scheme can allow the organization to improve its information security status.

It is planned to focus further research on expanding and integrating the SIEM system with a Security Orchestration, Automation, and Response (SOAR) system. This step aims to further enhance effectiveness and automate the response processes to potential threats and information security incidents. The integration of SIEM and SOAR can help achieve greater compliance with security requirements and ensure rapid and coordinated response to potential threats to the organization's information assets.

References

[1] R. Leszczyna, "Review of cybersecurity assessment methods: Applicability perspective," *Computers & Security,* vol. 108, 102376, 2021. https://doi.org/10.1016/j.cose.2021.102376.

[2] G. Wangen, C. Hallstensen and E. Snekkenes, "A framework for estimating information security risk assessment method completeness: Core Unified Risk Framework, CURF," *International Journal of Information Security*, vol. 17, pp. 681-699, 2018. https://doi.org/10.1007/s10207-017-0382-0.

[3] R. Leszczyna, "Standards on cyber security assessment of smart grid," *International Journal of Critical Infrastructure Protection*, vol. 22, pp. 70-89, 2018. https://doi.org/10.1016/j.ijcip.2018.05.006.

[4] Q. S. Qassim, N. Jamil, M. Daud, A. Patel and N. Ja'affar, "A review of security assessment methodologies in industrial control systems," *Information and Computer Security*, vol. 27, no. 1, pp. 47-61, 2019. https://doi.org/10.1108/ICS-04-2018-0048.

[5] N. A. Abu Othman, A. A. Norman and M. L. Mat Kiah, "Systematic literature review of security control assessment challenges," *Proceedings of the 2022 IEEE 12th International Conference on Control System, Computing and Engineering (ICCSCE)*, Penang, Malaysia, 2022, pp. 31-36. https://doi.org/10.1109/ICCSCE54767.2022.9935661.

[6] E. W. N. Bernroider, S. Margiol and A. Taudes, "Towards a general information security management assessment framework to compare cyber-security of critical infrastructure organizations," *Lecture Notes in Business Information Processing*, vol. 268, pp. 127-141, 2016. https://doi.org/10.1007/978-3-319-49944-4_10.

[7] J. Zuo, Z. Guo and Y. Lu, "An information security evaluation model

supporting measurement model adaptation," *Proceedings of the 2020 Int. Wirel. Commun. Mob. Comput. IWCMC*, 2020, pp. 1435-1439, https://doi.org/10.1109/IWCMC48107.2020.9148083.

[8] A. Georgiadou, M. Spiros, and A. Dimitrios, "Towards assessing critical infrastructures cyber-security culture during Covid-19 crisis," *A Tailor-Made Survey*. 2020, pp. 71-80. https://doi.org/10.5121/csit.2020.101806.

[9] Z. Sun, J. Zhang, H. Yang and J. Li, "Research on the effectiveness analysis of information security controls," *Proceedings of the 2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)*, Chongqing, China, 2020, pp. 894-897, https://doi.org/10.1109/ITNEC48623.2020.9084809.

[10] ISO/IEC 27004:2016. Information Technology. Security methods. Information security management. Monitoring, measurement, analysis and evaluation. [Online]. Available at: https://www.iso.org/standard/64120.html.

[11] A. Cadena, F. Gualoto, W. Fuertes, L. Tello-Oquendo, R. Andrade, F. Tapia, and J. Torres, "Metrics and indicators of information security incident management: A systematic mapping study," In: Rocha, Á., Pereira, R. (eds) Developments and Advances in Defense and Security. Smart Innovation, Systems and Technologies, 2019, vol. 152, pp. 507-519. Springer, Singapore. https://doi.org/10.1007/978-981-13-9155-2_40.

[12] R. Diesch and H. Krcmar, "SoK: linking information security metrics to management success factors," *Proceedings of the 15th International Conference on Availability, Reliability and Security (ARES'20). Association for Computing Machinery,* New York, NY, USA, Article 98, 2020, pp. 1–10. https://doi.org/10.1145/3407023.3407059.

[13] A. I. Al-Darwish and P. Choe, "A framework of information security integrated with human factors," *In: Moallem, A. (eds) HCI for Cybersecurity, Privacy and Trust. HCII 2019*. Lecture Notes in Computer Science, vol. 11594, 2019. Springer, Cham. https://doi.org/10.1007/978-3-030-22351-9_15.

[14] S. F. Aboelfotoh and N. A. Hikal, "A review of cyber-security measuring and assessment methods for modern enterprises," *JOIV: International Journal on Informatics Visualization*, vol. 3, issue 2, pp. 157-176, 2019. http://dx.doi.org/10.30630/joiv.3.2.239.

[15] Š. Orehek and G. Petrič, "A systematic review of scales for measuring information security culture," *Information and Computer Security,* vol. 29, no. 1, pp. 133-158, 2021. https://doi.org/10.1108/ICS-12-2019-0140.

[16] A. Erulanova, G. Soltan, A. Baidildina, M. Amangeldina and A. Aset, "Expert system for assessing the efficiency of information security," *Proceedings of the 2020 7th International Conference on Electrical and Electronics Engineering (ICEEE),* Antalya, Turkey, 2020, pp. 355-359. https://doi.org/10.1109/ICEEE49618.2020.9102555.

[17] S. Khan and S. Parkinson, "Review into state of the art of vulnerability assessment using artificial intelligence," *Guide to Vulnerability Analysis for Computer Networks and Systems*, Springer 2018, pp. 3-32, https://doi.org/10.1007/978-3-319-92624-7_1.

[18] V. A. Savchenko and O. D. Shapovalenko, "The main areas of application of artificial intelligence technologies in cyber security," *Modern Information Protection,* no. 4(44), pp. 6-11, 2020. (in Ukrainian). https://doi.org/10.31673/2409-7292.2020.040611.

[19] S. Lehominova, Y. Shchavinsky, T. Muzhanova, D. Rabchun, and M. Zaporozhchenko, "Application of sentiment analysis to prevent cyberattacks on objects of critical information infrastructure," *International Journal of Computing*, vol. 22, issue 4, pp. 534-540, 2023. https://doi.org/10.47839/ijc.22.4.3362.

[20] C. Schmitz, M. Schmid, D. Harborth and S. Pape, "Maturity level assessments of information security controls: An empirical analysis of practitioners assessment capabilities," *Computers & Security*, vol. 108, 102306, 2021. https://doi.org/10.1016/j.cose.2021.102306.

[21] B. Gomez, S. Vargas and J. P. Mansilla, "Maturity model of response protocols to ransomware scenarios in the mining sector," In: Guarda, T., Portela, F., Diaz-Nafria, J.M. (eds) Advanced Research in Technologies, Information, Innovation and Sustainability, *Proceedings of the ARTIIS 2023. Communications in Computer and Information Science*, vol. 1936, 2024, Springer, Cham. https://doi.org/10.1007/978-3-031-48855-9_20.

[22] E. F. Da Silva, R. M. de Barros, "Information security maturity model based on ISO 27001 for micro and small software development companies," *J. Inform. Syst. Eng. Manag*, vol. 4, issue 1, p. 10, 2019.

[23] L. Englbrecht, S. Meier and G. Pernul, "Towards a capability maturity model for digital forensic readiness," *Wireless Networks*, vol. 26, pp. 4895-4907, 2020. https://doi.org/10.3390/ijerph17031023.

[24] F. Y. H. García and L. Lema, "Model to measure the maturity of the risk analysis of information assets in the context of shipping companies," *RISTI - Iberian J. Inform. Syst. Technol.*, vol. 31, pp. 1–17, 2019. https://doi.org/10.17013/risti.31.1-17.

[25] B. Abazi, A. Kő, "A framework for semiautomatic risk assessment and a security maturity model based on ISO 27001," *J. Comput. Inform. Syst,* vol. 59, issue 3, pp. 264–274, 2019.

[26] D. Swift, "A practical application of SIM/SEM/SIEM automating threat identification," *SANS Institute,* 2021, 40 p. [Online]. Available at: https://sansorg.egnyte.com/dl/wGohjgzmXb.

[27] M. Cinque, D. Cotroneo and A. Pecchia, "Challenges and directions in security information and event management (SIEM)," *Proceedings of the 2018 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW)*, Memphis, TN, USA, 2018, pp. 95-99. https://doi.org/10.1109/ISSREW.2018.00-24.

[28] A. Sridharan and V. Kanchana, "SIEM integration with SOAR," *Proceedings of the 2022 International Conference on Futuristic Technologies (INCOFT),* Belgaum, India, 2022, pp. 1-6. https://doi.org/10.1109/INCOFT55651.2022.10094537.

[29] M. Kirsten, R. E. Freeman, "Some problems with employee monitoring," *Journal of Business Ethics*, vol. 43, issue 4, pp. 353–361, 2003. https://doi.org/10.1023/A:1023014112461.

[30] J. D. Bustard, "Ethical issues surrounding the asymmetric nature of workplace monitoring," In: Marinos, L., Askoxylakis, I. (eds) *Human Aspects of Information Security, Privacy, and Trust. HAS 2013, Lecture Notes in Computer Science*, vol 8030, 2013, Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-39345-7_24.

[31] B. Jendruszak, "*What is User Activity Monitoring (UAM)? Examples and best practices*," [Online], Available at: https://seon.io/resources/user-activity-monitoring/

[32] *2022 Magic Quadrant™ for SIEM released by Gartner® - LogRhythm Responds with New Cloud-Native Offering*, [Online], Available at: https://logrhythm.com/blog/2022-gartner-magic-quadrant-siem-logrhythm-responds-with-cloud-native-offering/

***Svitlana LEHOMINOVA,** Doctor of Economic Sciences, a Professor, Head of Department of Information and Cyber Security Management of the State University of Information and Communication Technologies. Scientific interests: economic security of the state, training of cyber security specialists, development of scientific methods of information and cyber security management.*

***Mykhailo ZAPOROZHCHENKO,** an Assistant of the Department of Information and Cyber Security Management of the State University of Information and Communication Technologies. Scientific interests: cyber security management processses, methods of risk assessment in the field of information protection in organizations, formation of competence of cyber security specialists, improvement of technical cyber security systems.*

YURII SHCHAVINSKY, *PhD, associate professor, Associate Professor of the Department of Information and Cyber Security Management of the State University of Information and Communication Technologies. Scientific interests: automated control systems, cyber security, information security, sentiment analysis, neural networks, artificial intelligence.*

Tetiana MUZHANOVA, *PhD, an Associate Professor of the Department of Information and Cyber Security Management of the State University of Information and Communication Technologies. Scientific interests: application of scientific methods of managing information and cyber security of the state, training of cyber security specialists.*

Vitalii TYSHCHENKO, *Assistant of the department, Department of Information and Cyber Security Management of the State University of Information and Communication Technologies. Scientific interests: information security, neural networks, countering false information*

Matvii Yushchenko, *Master's student of the Department of Information and Cyber Security Management of the State University of Information and Communication Technologies. Scientific interests: technical systems of cyber security, management of cyber security of banks, application of monitoring systems in cyber security, improvement of the cyber security system of organizations.*