A Method for Calculating Efficiency Indicators of Information Security Systems

Ihor Kozubtsov[1], Oleksii Silko[2], Lesia Kozubtsova[3]
Kruty Heroes Military Institute of Telecommunications and Information Technology
Kyiv, Ukraine
Ihor_kozubtsov@viti.edu.ua[1], oleksiy.silko@viti.edu.ua[2], lesia.kozubtsova@viti.edu.ua[3]

Mahmood Jawad Abu-AlShaeer
Al-Rafidain University College
Baghdad, Iraq
dean@ruc.edu.iq

Laith S. Ismail
Al-Turath University College
Baghdad, Iraq
laith.sabaa@turath.edu.iq

Mustafa Mohammmed Jassim
Al-Noor University College
Nineveh, Iraq
mustafa30@alnoor.edu.iq

***Abstract*—Background: As information and communication systems become more sophisticated and linked, there is an increasing demand for adequate information security and cybersecurity measures. The modern age necessitates a methodical approach to evaluating and fortifying these systems against emerging cyber threats.**

Objective: This study provides a unique technique for assessing the effectiveness of information security and cybersecurity solutions. The technique tries to discover and correct possible vulnerabilities by examining individual indications, providing enterprises with a data-centric strategy to enhance their cyber defenses.

Methods: The approach uses a large dataset from many firms and industries. To illustrate critical security components, key performance indicators (KPIs) such as incident response time, threat detection rates, and vulnerability repair were chosen. Advanced statistical approaches and machine learning algorithms were used to evaluate the effectiveness of these systems against set KPI criteria.

Results: The current study yields significant insights into the strengths and limitations of various security techniques. By evaluating specific indicators, opportunities for improvement were found, allowing firms to focus their security operations more effectively. The study validated the influence of system complexity and security investment on overall system efficiency.

Conclusion: This article proposes a data-driven strategy to improve the efficiency of information and cybersecurity systems, providing companies with a road map for protecting their essential assets and data in the face of an ever-changing cyber threat scenario.

I. Introduction

Information and communication systems (ICS) security has become a significant problem in our ever-linked global environment. The acquisition and use of information are vital for contemporary enterprises, and the increasing dependence on digital platforms has rendered them susceptible to a diverse range of cyber dangers. Cyberattacks' increasing magnitude and complexity need adequate information security and cybersecurity measures, making their significance more crucial than ever before [1].

This article presents a thorough technique to solve the urgent issue of analyzing individual indicators inside Information and Communication Systems (ICS). The security of Industrial Control Systems (ICS) is a multifaceted domain that comprises several interconnected elements, such as technological components, operational procedures, human actions, and the continuously changing landscape of potential threats. This technique analyzes and evaluates these components, offering firms a comprehensive strategy to improve their efficiency in information security and cybersecurity [2].

In an era characterized by the potential for severe repercussions resulting from cyber-attacks, it is essential to comprehend the intricate aspects of information security. Implementing robust firewalls and antivirus software is not the main focus; a comprehensive examination of several contributing elements is required [3]. The approach used in this study acknowledges the need for proactive, adaptive, and responsive information security measures in effectively addressing the ever-changing landscape of cyber threats [4].

The field of cybersecurity has seen significant transformation during its development. In contemporary times, the significance of this matter extends beyond the realm of information technology. It assumes a crucial role as a strategic imperative encompassing several facets of organizational operations. In contemporary times, cyberattacks have gone beyond the boundaries of the digital domain. They are capable of causing significant disruptions to vital infrastructure, compromising the security of sensitive information, and inflicting harm upon an organization's reputation. Hence, it is crucial to use a systematic and comprehensive strategy when evaluating indications of information security [5].

One crucial factor that this technique considers is the human element. Numerous studies have shown that many security breaches may be attributed to human mistakes or neglect. Organizations may mitigate the risk of insider threats and mistakes by establishing a security culture by assessing various indicators of human behavior, training, and awareness [6].

Information security is fundamentally reliant on technology. The present study presents a technique that offers a structured approach to evaluating the efficacy of technical protections, including firewalls, intrusion detection systems, and encryption approaches. The evaluation process considers the most recent breakthroughs in cybersecurity technology and assesses their fit with an enterprise's unique requirements.

Process assessment is an essential component of this technique. Organizations must possess well-defined, flexible security processes and incident response strategies [7]. By examining specific indicators linked to several processes, this technique facilitates the identification of vulnerabilities, deficiencies, and opportunities for improvement. Consequently, this capability empowers firms to improve their entire security stance.

The dynamic nature of the threat environment necessitates continuous adaptation since new attack vectors often arise. Consequently, firms must be updated on current cybersecurity trends and risks. [8]. Our technique emphasizes the crucial role of monitoring and information collecting within an organization's proactive security plan.

This article presents a novel technique that effectively tackles the complex aspects of information security and cybersecurity in Information and Communication Systems (ICS). Organizations may efficiently increase their security posture and safeguard critical assets by evaluating individual indicators within technology, human behavior, procedures, and threat intelligence.

The subsequent parts will explore the constituent elements and procedures of the technique, as well as elucidate how businesses might include it to enhance their efficacy in information security and cybersecurity. This methodology presents a comprehensive strategy for protecting the integrity, confidentiality, and availability of digital information in the current era characterized by persistent cyber threats. DoingDoing guarantees organizations' ongoing prosperity and resilience in light of the ever-changing nature of cyber threats.

A. Problem statement

The efficiency of a system is a property of a system that characterizes its ability to perform its efficiency function (EF).

The information security and cyber security system (ISCSS) is a comprehensive combination of software, cryptographic, organizational, and other tools, techniques, and procedures to safeguard information and cyber security. It should be noted that ISCSS is a relatively new system. Therefore, it is advisable to study the issues of its efficient functioning to develop a mathematical apparatus for its evaluation.

By the "efficiency of the information security and cyber security system" (E_S), we will understand the degree of compliance of the results achieved with the set goals for information protection.

An efficiency indicator is a value that characterizes the degree to which the system has achieved any of its assigned tasks. Therefore, the head of the department where the information and communication system (ICS) is located is obliged to make timely and adequate decisions on changes to the security policy based on an audit (evaluation) of the data protection and cybersecurity system's efficiency. Thus, the basis for solving this priority scientific and technical task is the operational goal "1.5. Improvement of the cyber security and information security system" of the Strategic Defense Bulletin [9] in the security and defense sector of Ukraine, Law of Ukraine "On the Basic Principles of Ensuring Cyber Security of Ukraine"[10], Cyber Security Strategy of Ukraine [11], "Decision of the National Security and Defense Council of Ukraine"[12].

B. Aim of the Article

This article aims to define and justify the structure and content of the critical processes involved in calculating and assessing the effectiveness levels of information security and cybersecurity systems inside Information and Communication Systems (ICS). The emphasis is on examining specific partial indications, which are critical in establishing the overall efficacy of various security measures.

This study aims to shed light on assessing information security and cybersecurity systems using a data-driven approach by offering a thorough methodology. The importance of examining particular partial indicators that contribute to the overall resilience of the security system is emphasized in the article.

The article gives significant insights into the strengths and shortcomings of the security system in ICS via a detailed evaluation of these partial indicators. Organizations should prioritize enhancing their security measures by knowing these essential characteristics.

II. Literature Review

Scientific search and analysis of publications in which the authors investigated the chosen area made it possible to assert that the study task is new.

The authors made the first attempts to calculate the efficiency of the information system security system for a fundamentally new system in a scientific article [13]. For the calculation, we used the formula for the ratio of the obtained effect achieved during the implementation of the ISCSS to the total costs of acquisition, installation, configuration, maintenance, and support. It should be noted that in this way, it is approximate and challenging to calculate the effectiveness of the ISCSS.

In works [14], [15], the authors use a mathematical model for evaluating the system's efficiency according to the loss prevention criterion. Information security costs should be efficient if they ensure compliance with the requirements of regulatory documents, standards adopted by the state, and the organization's information security concept. So, loss prevention is the difference between losses before and after the implementation of measures aimed at improving the level of information or cyber security and generally reflects the part of the profit that could have been lost.

If the system's efficiency is considered as a property of the system that characterizes its ability to perform its efficiency function, then to a certain extent, it is possible to evaluate its efficiency through the indicator of functioning stability in destructive influences conditions. This approach is used in the works [16], [17], [18]

Further development of the theory and practice of evaluating the efficiency of the system was acquired in works for a partial case, namely: evaluating the efficiency of measures to ensure cyber security of objects of critical information infrastructure of organizations [19]; calculating the ISCSS efficiency indicators [20]; supporting individual indicators to determine the ability of the ISCSS to store data in unique conversation systems for information and communication [21]; justifying individual metrics for evaluating the ISCSS of objects of vital information infrastructure of organizations [22].

Therefore, the set of academic works [5-14] logically and purposefully brought the issue of supporting the approach used for estimating the effectiveness of the data assurance and security measures system in communication and information systems and assessing individual indicators closer to resolution.

III. METHODOLOGY

Efficiency evaluation is a procedure aimed at determining qualitative and quantitative efficiency indicators, identifying critical elements of the system, and determining the integral efficiency indicator of the system as a whole.

Our methodology entails using Microsoft Excel to evaluate the effectiveness of Information Security and Cyber Security Systems (ISCSS). The selection of Excel is based on its wide availability, flexibility, and ability to handle complex calculations and visualizations, which are essential for effectively assessing cybersecurity metrics.

The Excel system is organized across many matrices, representing different ISCSS efficiency facets. These matrices are shaped by prior research in the field. The Personnel Staffing Matrix is derived from the technique outlined by D. Timpson and E. Moradian [4], which was influenced by the study undertaken by Khlaponin et al. [27]. This matrix displays a juxtaposition of the current and projected staffing levels for different positions within the cybersecurity team, offering a quantifiable assessment of staffing adequacy in terms of percentages.

The Cybersecurity Control Matrix, built from the concepts introduced by Y. You et al. [1], is a significant element. The matrix evaluates the cybersecurity measures' effectiveness by assigning them scores based on a pre-established scale. In addition, the Risk Assessment Matrix, as referenced by H. Suryotrisongko and Y. Musashi [7], aligns with strategic defense bulletins and cybersecurity policies [9], [10], [11]. The process includes categorizing risks, assessing their likelihood and impact, and devising strategies to mitigate them.

The Efficiency Indicator Matrix combines data from various matrices to compute crucial efficiency indicators. This research integrates many variables, including incident reaction time, resolution rate of cybersecurity concerns, and the cost-effectiveness of implemented solutions, based on the methodologies of N. A. Maslova [13] and K. A. Andrieiev [14].

The system employs charts and graphs to graphically depict data, facilitating an intuitive understanding of ISCSS performance. This visual approach aligns with the methodologies emphasized by Kozubtsova et al. [19], [20], [21], [22], which stress the accessibility and comprehensibility of efficiency indicators and cybersecurity metrics.

The Excel-based solution proves its practical effectiveness by offering precise and actionable insights into the operation of ISCSS. This exemplifies the integration of theoretical analysis and practical application in assessing the efficacy of cybersecurity, in line with the research undertaken by Zabara and Kozubtsova [23] and L. M. Kozubtsova [24]. This system is a comprehensive and practical tool for organizations to evaluate and enhance cybersecurity protocols.

Based on the work [20], [23] on calculating efficiency indicators for the functioning of the information security and cyber security system, it is proposed to construct a logical sequence for evaluating the efficiency of the ISCSS in the future methodology (Fig. 1).

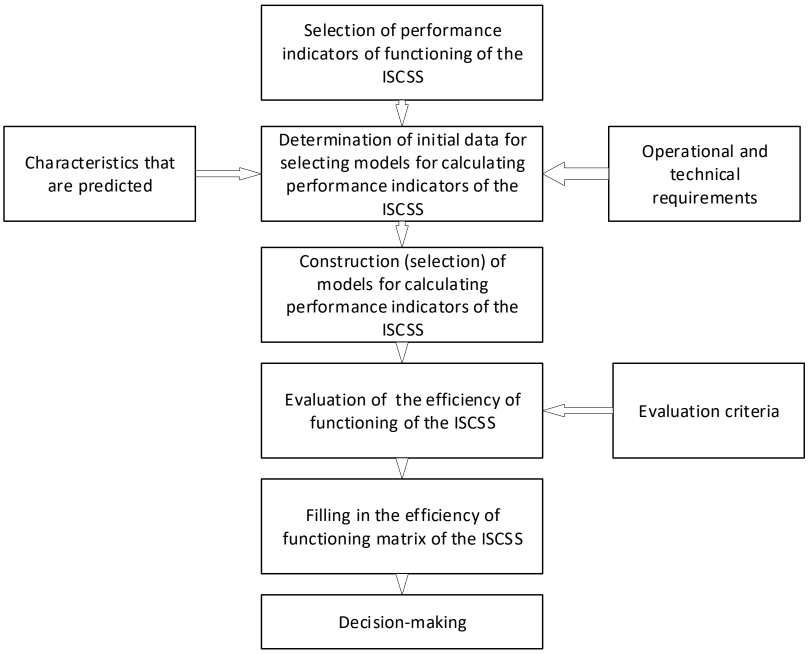

Selection of performance indicators of functioning of the ISCSS
Characteristics that are predicted
Determination of initial data for selecting models for calculating performance indicators of the ISCSS
Operational and technical requirements
Construction (selection) of models for calculating performance indicators of the ISCSS
Evaluation of the efficiency of functioning of the ISCSS
Evaluation criteria
Filling in the efficiency of functioning matrix of the ISCSS
Decision-making

Fig. 1. Sequence of evaluation of the ISCSS efficiency

TABLE II. KEY SYMBOLS AND TERMS IN ISCSS EFFICIENCY EVALUATION

Symbol/Term	Definition
IS CSS	Information Security and Cyber Security System
ICS	Information and Communication Systems
E_U	IS CSS Equipping Coefficient with Cyber Defense Means; measures the system's protection against cyber-attacks
E_TG	IS CSS Technical Readiness Coefficient: shows the functional readiness of the system's cybersecurity mechanisms.
E_US	IS CSS Equipping Coefficient with Serviceable Cyber Defense Means indicates the level of practical cyber defense tools in the network.
E_K	IS CSS Staffing Coefficient with IT System Administrators; represents the number of IT system managers on staff.
E_HP	IS CSS Staffing Coefficient with Service Personnel; indicates the staffing level of the system's service personnel
E	Composite Efficiency Indicator: the mean of the five subpart efficiency indicators for an overall assessment of system performance
EF	Efficiency Function: a property characterizing the system's ability to perform efficiently
PKZ	Cybersecurity Indicator: evaluates the system's cybersecurity level
KUZ	Equipping the Coefficient of ISCSS in ICS with Cyber Defense Means
KTGZ	Technical Readiness Coefficient of ISCSS Cyber Defense Means in ICS
KUSZ	Equipping the Coefficient of ISCSS in ICS with Serviceable Cyber Defense Means
KCA	Staffing Coefficient of ISCSS in ICS with IT System Administrators
KOP	Staffing Coefficient of ISCSS in ICS with Service Personnel
PKZPT(S)	Cybersecurity of ISCSS in ICS based on Penetration Testing Results

Stage 1 preparation of initial data.

Selection of a specific ISCSS in the ICS to evaluate its efficiency.

The initial data for the calculation is the state of availability of serviceable (suitable for use for its intended purpose) cyber defense, which means the need for regular operation in case of collapse.

We will accept the following assumptions and limitations in our work:

- the actions of factors that determine the survivability, reliability, anti-interference capability, and cyber security of ISCSS cyber defense means in the ICS are considered independent;
- technical reliability of the ISCSS cyber defense means we assume $P_{\text{TN}} = 1$ in the ICS.

Stage 2. Selection of indicators and criteria for evaluating the efficiency of the ISCSS in the ICS based on the available initial data.

The methodology development requires a reasonable choice of individual partial indicators of the functioning of the ISCSS in the ICS as partial performance indicators. For our study, we use the indicators justified in [22], taking into account the requirements for the efficiency indicator:

- have a certain physical inventory; be suitable for quantitative analysis;
- have a simple and convenient shape;
- reflect one of the significant aspects of the system's functioning;
- provide the required sensitivity.

Partial efficiency indicators of the ISCSS in the ICS reflect one of the significant aspects of the system's functioning.

Following Stage 2 above, we propose the following partial indicators of efficiency (E_{P}) as numerical values that will characterize the degree of achievement of the ISCSS in the ICS of the tasks assigned to it:

- cyber security (P_{KZ});
- equipping coefficient of the ISCSS in the ICS with cyber defense means (K_{UZ});
- technical readiness coefficient of the ISCSS in the ICS of cyber defense means (K_{TGZ});
- equipping coefficient of the ISCSS in the ICS with serviceable cyber defense means (K_{USZ});
- staffing coefficient of the ISCSS in the ICS with information technology system administrators (K_{CA});
- staffing coefficient of the ISCSS in the ICS with service personnel (K_{OP});
- cyber security of the ISCSS in the ICS based on the results of penetration testing ($P_{\text{KZ}}^{\text{PT}}(S)$).

By "means of cyber defense of information," we will understand the software, hardware program, and hardware means intended for cyber defense.

The generalized efficiency indicator of the ISCSS in the ICS combines partial indicators.

If no calculation was performed for an individual indicator, then the corresponding values are not substituted in the calculation formula (3), and the conclusions give a short and concise justification for why a particular indicator was not used [24]

The efficiency criteria of the ISCSS in ICS can be many, but the choice of specific ones depends on the specifics of the evaluation and is more related to the compliance of the technical condition class of the ISCSS components with the level of functioning quality.

The scheme of compliance of the technical condition class of components of the ISCSS in the ICS with the quality level is shown in Fig. 2, developed in work [25], [26] and adapted for the partial case of evaluating the efficiency of the ISCSS.

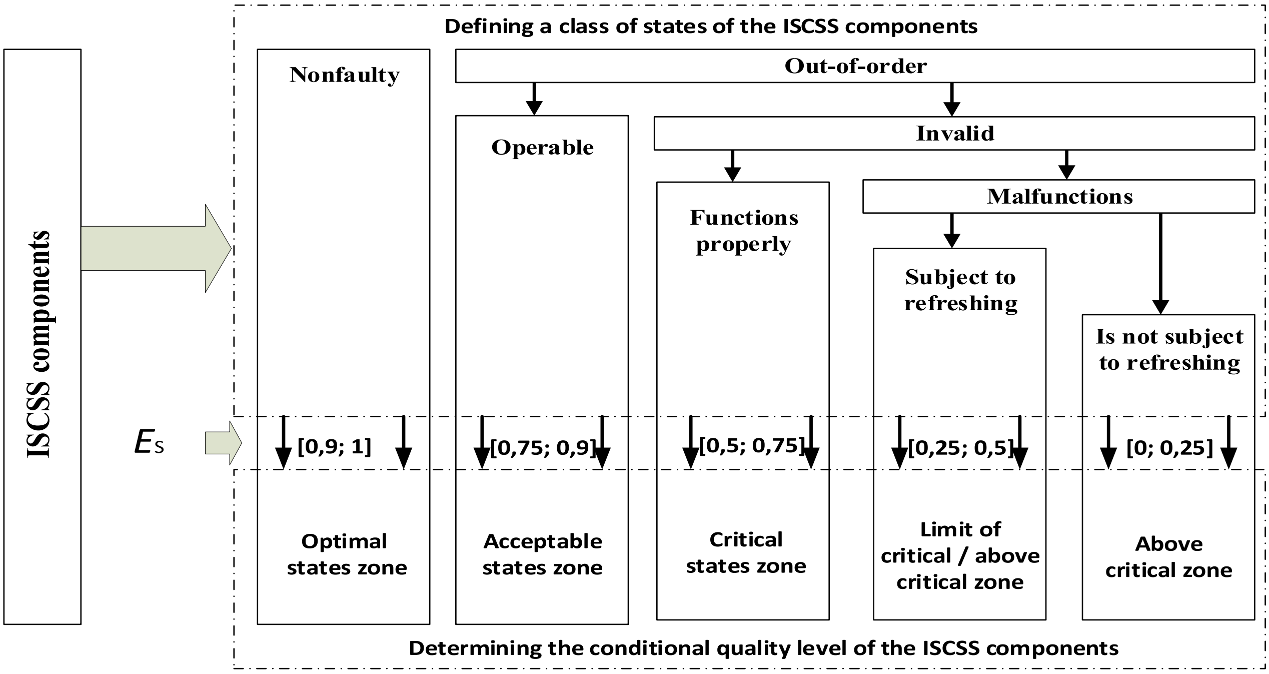


Fig. 2. Scheme of compliance of the class of technical condition of the ISCSS components with the level of quality of functioning

Thus, the criteria for evaluating the efficiency of the ISCSS in the ICS according to the generalized indicator are presented in (Table I).

Stage 3. Calculation of efficiency indicators of the ISCSS in the ICS based on the results of a passive audit of complex indicators.

Stage 3.1 Calculation of cyber security provided by the ISCSS in the ICS.

The mathematical model for calculating the efficiency of the ISCSS in the ICS by the cyber security indicator (P_{KZ}) can be represented by the following approximate ratio (3):

$$Es \approx \mathrm{P}KZ, \tag{3}$$

We omit the total calculation of cyber security for the ISCSS in the ICS since the method is similar and described in detail in the work [16].

TABLE I. CRITERIA FOR EVALUATING THE EFFICIENCY OF THE ISCSS ACCORDING TO THE GENERALIZED INDICATOR

Criteria E_C	Level	Linguistic description	
0 ≤ E_S ≤0,25	unsatisfactory (UNS)	ISCSS in the ICS is invalid and must be fully refreshed	Possible leak of information from the ICS
0,25<E_S ≤0,5	low (L)	ISCSS in the ICS is subject to refreshing	Creating conditions for information leakage from ICS
0,5<EC ≤0,75	average(A)	ISCSS in the ICS functions properly	ISCSS provides guaranteed information protection and cybersecurity in the ICS
0,75<E_S ≤0,9	high (H)	ISCSS in the ICS is operable	
0,9<E_S ≤1	highest (HI)	ISCSS in the ICS is nonfaulty	

Stage 3.2 Calculate the equipping coefficient of the ISCSS in the ICS with cyber defense means.

$$K_{UZ} = \frac{N_z^f}{N_Z}, \tag{4}$$

To calculate the equipping coefficient of the ISCSS in the ICS with cyber defense means, we apply the following ratio (4):

Where K_{UZ} – equipping coefficient of the ISCSS in the ICS with cyber defense means;

N – staffing of cyber defense means;

N_z^f is the actual number of cyber defenses available.

Stage 3.3 Calculate the coefficient of technical readiness of cryptographic information protection means, technical information protection, and cybernetic protection.

The coefficient of technical readiness of cyber defense means is calculated using the formula (5):

$$K_{TGZ} = \frac{N_Z^S}{N_Z^f}, \tag{5}$$

where K_{TGZ} – coefficient of technical readiness of cyber defense means of the ISCSS in the ICS;

N_Z^S– number of serviceable cyber defense means in the ISCSS in the ICS;

N_Z^f – the actual number of cyber defenses means available.

Stage 3.4 Calculate the equipping coefficient of the ISCSS in the ICS with serviceable means of cryptographic information protection, technical information protection, and cybernetic protection.

Calculation of the equipping coefficient of the ISCSS in the ICS with serviceable cyber defense means is calculated by the formula (6):

$$K_{USZ} = K_{UZ} \times K_{TGZ} = \frac{N_Z^f}{N_Z}, \qquad (6)$$

where K_{USZ} – equipping coefficient of the ISCSS in the ICS with serviceable cyber defense means;

K_{UZ} – equipping coefficient of the ISCSS in the ICS with cyber defense means;

K_{TGZ} – coefficient of technical readiness of cyber defense means;

N_Z^f– – number of serviceable cyber defense means;

N_Z – staffing of cyber defense means.

Stage 3.5 Calculation of the staffing coefficient of the ISCSS with information technology system administrators

Step 3.5 Calculation of the staffing coefficient of the ISCSS with information technology system administrators is calculated using the formula (7):

$$K_{CA} = \frac{L_{CA}^f}{L_{CA}}, \qquad (7)$$

where K_{CA} – staffing coefficient of the ISCSS in the ICS with ISCSS information technology system administrators;

L_{CA} – staffing of information technology system administrators of cyber defense means of the ISCSS in the ICS;

L_{CA}^f – the actual number of information technology system administrators of cyber defense means of the ISCSS in the ICS available;

Stage 3.6 Calculation of the coefficient of staffing of the ISCSS in the ICS of full-time positions by service personnel.

Calculation of the coefficient of staffing of full-time positions of the ISCSS in the ICS by service personnel is carried out according to the formula (8):

$$K_{OP} = \frac{L_{OP}^f}{L_{OP}}, \qquad (8)$$

where K_{OP} – coefficient of staffing of full-time positions of the ISCSS in the ICS by ISCSS service personnel;

L_{OP} – staffing of the service personnel of cyber defense means;

L_{OP}^f is the actual number of service personnel available in cyber defense means.

Stage 4 Calculation of cyber security based on the results of an external (active) audit.

Calculate cyber security based on the results of an external (active) audit (detected active threats based on penetration testing results). This approach aims to control the cyber security of the ICS means and their components as of the moment in time t_{DIV1}, under the conditions of actions of test destructive information influences (DII) when F_{DII} =1. Suppose the ISCSS contains means (components) of active counteraction to cyber influences (DII). In that case, the calculation $P_{\mathrm{KZ}}(S)$ is carried out using indicators of successful and unsuccessful attempts to disrupt the normal functioning of the specified means.

The cyber security $\mathrm{P}KZ(S)$ of the system S is calculated using the formula (9):

$$\mathrm{P}KZ(S) = 1 - \frac{\mathrm{N}_{\mathrm{DIV}}^{\mathrm{B}}(\mathrm{S})}{\mathrm{N}_{\mathrm{DIV}}^{\mathrm{Z}}(\mathrm{S})}, \qquad (9)$$

where $\mathrm{N}_{\mathrm{DIV}}^{\mathrm{Z}}(\mathrm{S})$ – total number of DII performed aimed at the entire system S;

$\mathrm{N}_{\mathrm{DIV}}^{\mathrm{B}}(\mathrm{S})$ is the number of successful attempts to implement DII on the entire system S and is based on the results of notification by the incident recording system.

Stage 5 Generalization of the results of calculating the efficiency of the ISCSS in the ICS.

To find a generalized indicator of the efficiency of the ISCSS in the ICS, we use the formula (10):

$$E_S = \frac{P_{KZ} + P_{UZ} + P_{USZ} + P_{TGZ} + P_{CA} + P_{OP} + P_{KZ}^{PT}(S)}{N_P}, \qquad (10)$$

where N_{P} is the number of partial indicators of efficiency of the ISCSS in the ICS involved in the calculation.

Stage 6 Evaluation of the efficiency level of the ISCSS in the ICS.

Evaluation of the efficiency level of the ISCSS in the ICS is carried out by comparing the obtained calculated value from the area in which it fell in the following Table I.

Stage 7 Evaluating the impact of the value of each partial indicator on the overall value of the efficiency level of the ISCSS in the ICS.

The purpose of applying this stage is for the administrator to analyze the contribution of each partial indicator to the overall value of the efficiency level of the ISCSS in the ICS.

If necessary, a partial indicator is adjusted to achieve the maximum generalized value of the efficiency of the ISCSS in the ICS.

The approximate (critical) contribution of individual (partial) efficiency indicators to the generalized indicator of the efficiency of the ISCSS in the ICS is presented in Table III. The squares located at the intersection of the corresponding rows and columns indicate the calculated partial indicator's ability to influence the corresponding efficiency E_{C}.

TABLE III. EVALUATION CRITERIA OF INDIVIDUAL (PARTIAL) EFFICIENCY INDICATORS E_P FOR A GENERALIZED INDICATOR OF THE EFFICIENCY OF THE ISCSS IN THE ICS

Evaluation criteria	Individual (partial) efficiency indicator (E_{pi})				
	$0 \le E_p \le 0{,}25$	$0{,}25 < E_p \le 0{,}5$	$0{,}5 < E_p \le 0{,}75$	$0{,}75 < E_p \le 0{,}9$	$0{,}9 < E_p \le 1$
$0 \le E_S \le 0{,}25$	UNS	UNS	UNS	UNS	UNS
$0{,}25 < E_S \le 0{,}5$	L	L	L	L	L
$0{,}5 < E_S \le 0{,}75$	A	A	A	A	A
$0{,}75 < E_S \le 0{,}9$	A	A	A	H	H
$0{,}9 < E_S \le 1$	H	H	H	H	HI

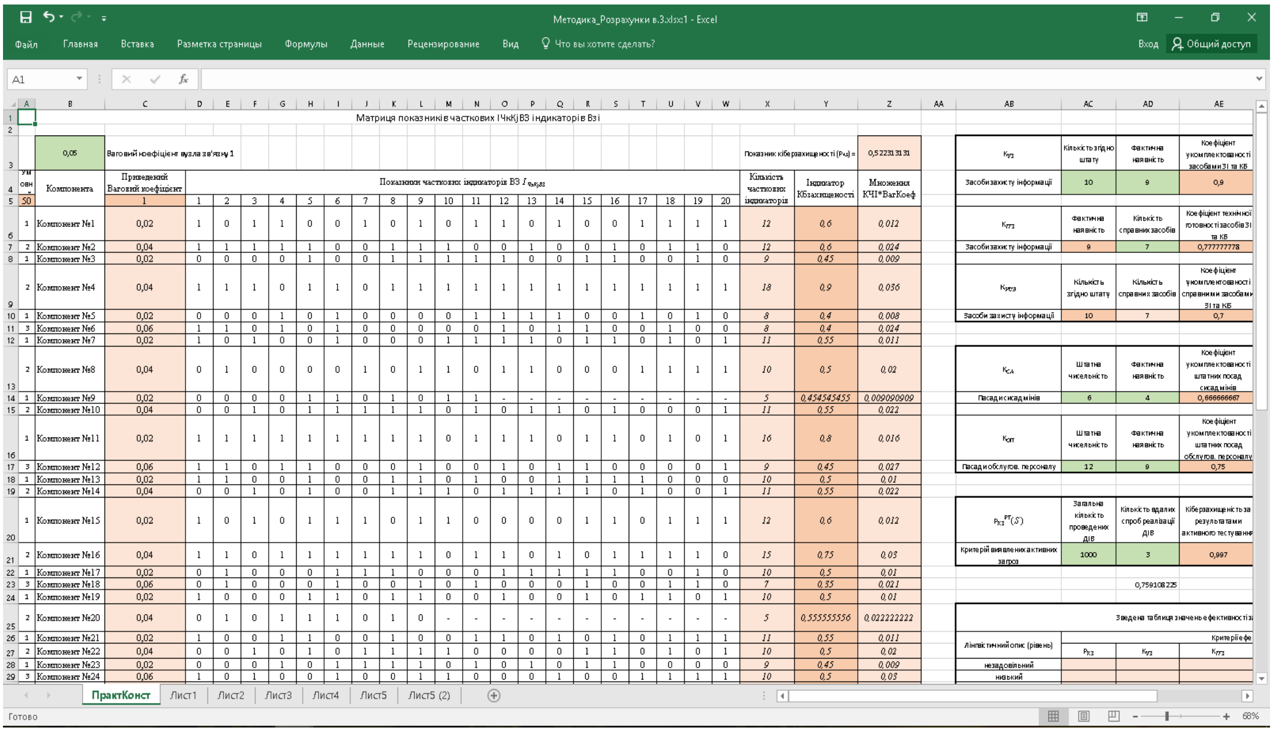
IV. RESULTS

Our study findings are mainly concerned with the practical application of the suggested methodology for assessing the effectiveness of information security and cybersecurity systems (IS CSS) in information and communication systems (ICS). We implemented the approach in Microsoft Excel, which enabled us

to run calculations based on the primary data and provide both intermediate and ultimate efficiency indicators.

The technique was developed using Microsoft Excel, a widely accessible and frequently used software program that makes it simple for organizations to execute the recommended methodology. The initial data is entered into an Excel spreadsheet, and the calculations outlined by the methodology are performed using Excel's built-in functions.

Fig. 3 shows the Excel spreadsheet for entering the first data. For each system being assessed, the starting data contains the overall number of cyber defense means, the number of operable cyber defense means, the number of system administrators, and the number of service employees.



Матриця показників часткових IЧкКjВЗ індикаторів Взі

0,05 Ваговий коефіцієнт вузла зв'язку 1

Показник кіберзахищеності (Pкз) = 0,522313131

Умовн.	Компонента	Приведений Ваговий коефіцієнт	Показники часткових індикаторів ВЗ $I_{ЧкКjВЗ}$																				Кількість часткових індикаторів	Індикатор КБзахищеності	Множення КЧІ*ВагКоеф
50		1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20			
1	Компонент №1	0,02	1	0	1	1	0	0	1	0	1	0	1	1	0	1	0	0	1	1	1	1	12	0,6	0,012
2	Компонент №2	0,04	1	1	1	1	1	0	0	1	1	1	0	0	1	0	0	1	0	1	1	0	12	0,6	0,024
1	Компонент №3	0,02	0	0	0	0	1	0	0	1	1	1	1	1	0	0	1	1	0	0	1	0	9	0,45	0,009
2	Компонент №4	0,04	1	1	1	0	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	18	0,9	0,036
1	Компонент №5	0,02	0	0	0	1	0	1	0	0	0	0	1	1	1	1	0	0	1	0	1	0	8	0,4	0,008
3	Компонент №6	0,06	1	1	0	1	0	1	0	0	0	0	0	1	0	1	1	0	0	1	0	0	8	0,4	0,024
1	Компонент №7	0,02	1	0	1	0	0	1	0	0	0	1	1	1	1	0	1	1	0	1	0	1	11	0,55	0,011
2	Компонент №8	0,04	0	1	0	0	0	0	1	0	1	1	0	1	1	0	0	0	1	1	1	1	10	0,5	0,02
1	Компонент №9	0,02	0	0	0	0	1	1	0	1	0	1	1	-	-	-	-	-	-	-	-	-	5	0,454545455	0,009090909
2	Компонент №10	0,04	0	0	1	0	1	1	1	1	1	0	1	0	1	1	0	1	0	0	0	1	11	0,55	0,022
1	Компонент №11	0,02	1	1	1	1	1	1	1	1	1	0	1	1	1	0	1	1	0	1	0	1	16	0,8	0,016
3	Компонент №12	0,06	1	1	0	1	1	0	0	0	1	0	0	1	0	1	1	0	0	0	0	1	9	0,45	0,027
1	Компонент №13	0,02	1	1	0	0	1	0	0	1	1	0	1	0	0	1	1	1	1	0	0	0	10	0,5	0,01
2	Компонент №14	0,04	0	0	1	0	1	0	0	1	1	1	0	1	1	1	1	0	1	0	0	1	11	0,55	0,022
1	Компонент №15	0,02	1	0	1	0	1	1	1	0	1	1	0	0	0	0	1	1	0	1	1	1	12	0,6	0,012
2	Компонент №16	0,04	1	1	0	1	1	1	1	1	1	0	1	1	0	1	0	1	1	1	1	0	15	0,75	0,03
1	Компонент №17	0,02	0	1	0	0	0	1	1	1	0	0	0	1	1	1	1	1	0	0	1	0	10	0,5	0,01
3	Компонент №18	0,06	0	1	0	0	0	1	0	0	1	0	1	0	0	0	1	0	0	1	1	0	7	0,35	0,021
1	Компонент №19	0,02	1	0	0	0	1	1	0	1	1	0	0	1	0	0	1	0	1	1	0	1	10	0,5	0,01
2	Компонент №20	0,04	0	1	0	1	1	1	0	1	0	-	-	-	-	-	-	-	-	-	-	-	5	0,555555556	0,022222222
1	Компонент №21	0,02	1	0	0	1	1	0	0	1	0	0	1	1	0	1	0	1	0	1	1	1	11	0,55	0,011
2	Компонент №22	0,04	0	0	1	0	1	0	1	1	1	1	0	0	0	0	1	1	0	1	0	1	10	0,5	0,02
1	Компонент №23	0,02	0	0	0	1	0	1	1	1	1	0	1	0	1	0	1	1	0	0	0	0	9	0,45	0,009
3	Компонент №24	0,06	1	0	1	0	0	1	0	0	1	1	0	0	0	1	0	0	1	1	1	1	10	0,5	0,03

Kуз	Кількість згідно штату	Фактична наявність	Коефіцієнт укомплектованості засобами ЗІ та КБ
Засоби захисту інформації	10	9	0,9

Kтгз	Фактична наявність	Кількість справних засобів	Коефіцієнт технічної готовності засобів ЗІ та КБ
Засоби захисту інформації	9	7	0,777777778

Kусз	Кількість згідно штату	Кількість справних засобів	Коефіцієнт укомплектованості справними засобами ЗІ та КБ
Засоби захисту інформації	10	7	0,7

Kса	Штатна чисельність	Фактична наявність	Коефіцієнт укомплектованості штатних посад сисадмінів
Пасади сисадмінів	6	4	0,666666667

Kоп	Штатна чисельність	Фактична наявність	Коефіцієнт укомплектованості штатних посад обслугов. персоналу
Пасади обслугов. персоналу	12	9	0,75

$P_{КЗ}^{PT}(S)$	Загальна кількість проведених ДІВ	Кількість вдалих спроб реалізації ДІВ	Кіберзахищеність за результатами активного тестування
Критерій виявлених активних загроз	1000	3	0,997

0,759108225

Зведена таблиця значень ефективності за

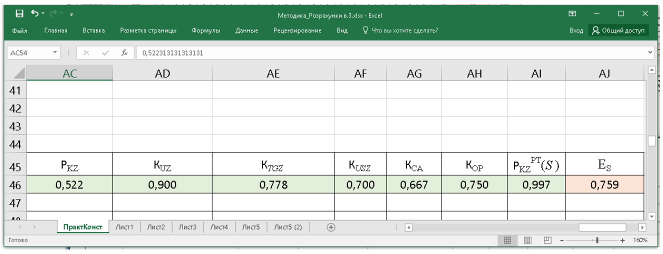
Лінгвістичний опис (рівень)	Критерії ефе		
	Pкз	Kуз	Kтгз
незадовільний			
низький			

Fig. 3. Fragment of calculating the efficiency of the ISCSS in the ICS using Microsoft Excel

After the data input, the Excel spreadsheet automatically calculates the various partial efficiency indicators for each system. These indicators include the equipping coefficient of the IS CSS with cyber defense means (E_U), the technical readiness coefficient of the IS CSS (E_TG), the equipping coefficient of the IS CSS with serviceable cyber defense means (E_US), the staffing coefficient of the IS CSS with IT system administrators (E_K), and the staffing coefficient of the IS CSS with service personnel (E_HP).

A composite efficiency indicator (E) is calculated for each system after calculating the partial efficiency indicators. The composite efficiency indicator is the average of the five partial efficiency indicators and provides a general measure of the system's efficiency.

Fig. 4 below shows the Excel spreadsheet with the intermediate results (the partial efficiency indicators) and the final result (the composite efficiency indicator) for each system.



	AC	AD	AE	AF	AG	AH	AI	AJ
41								
42								
43								
44								
45	P_{KZ}	K_{UZ}	K_{TGZ}	K_{USZ}	K_{CA}	K_{OP}	$P_{KZ}^{PT}(S)$	E_S
46	0,522	0,900	0,778	0,700	0,667	0,750	0,997	0,759
47								

Fig. 4. Fragment of calculating the efficiency of the ISCSS in the ICS using Microsoft Excel

A. Distribution Histograms of IS CSS Efficiency Indicators in ICS for 100 Systems

The generated histograms below represent the distributions of the calculated efficiency indicators for the Information Security and Cybersecurity Systems (IS CSS) in the Information and Communication Systems (ICS) for 100 systems.

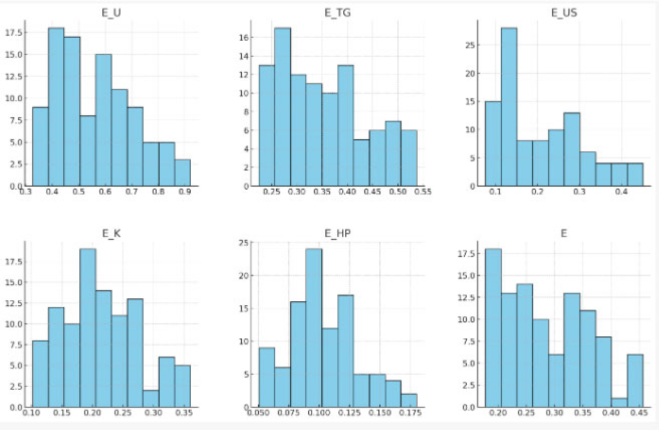


Fig. 5. Distribution of Calculated Efficiency Indicators for 100 IS CSS Systems

E_U (IS et al. with Cyber Defense Means): This indicates how well the system is protected against cyber-attacks, ranging between 0.35 and 0.7. This implies that while all systems possess a certain degree of security, a considerable part needs more complete readiness to safeguard against cyber-attacks. The possible consequence of this situation is twofold: firstly, systems with lesser security measures may face a greater vulnerability to breaches, and secondly, there may be an excessive dependence on a restricted range of Defense techniques. Organizations should expand their range of cybersecurity technologies to enhance this statistic, assuring a more assertive Defense posture.

E_TG (IS CSS technical readiness coefficient): This indication shows the functional readiness of the system's cyber security mechanisms; it ranges between 0.25 and 0.55. The observed distribution indicates a modest degree of preparedness across systems, with potential for improvement. The dispersion of this indicator reflects the degree of variation in the maintenance and updating of cybersecurity measures. In order to increase this coefficient, organizations must carry out frequent upgrades and thorough testing of their security architecture.

E_US (IS CSS Equipping Coefficient with Serviceable Cyber Defense Means): This metric shows the level by which the network is outfitted with practical cyber defense tools; it ranges between 0.05 and 0.4. This finding is crucial because it highlights a deficiency in the ability for operational cybersecurity. Organizations should audit their existing cybersecurity technologies to assess their efficacy and usability to prevent any vulnerabilities resulting from old or inadequate Defense mechanisms.

E_K (IS CSS staffing coefficient with IT system administrators): This metric shows the number of IT system managers on staff, ranging from 0.1 to 0.35. The allocation of resources in this context raises questions about the sufficiency of investment in human resources for cybersecurity. Sufficient human resources are essential for both the adoption and upkeep of cybersecurity measures, and organizations should prioritize investing in proficient workers to manage their IT systems efficiently.

E_HP (IS CSS Staffing Coefficient with Service Personnel): This indicator shows the system's service personnel staffing level; the value ranges between 0.05 and 0.15. It highlights the need for proficient personnel to address and handle cybersecurity breaches promptly. Organizations should reassess their employment arrangements and examine the need for ongoing employee training to strengthen their defense capabilities.

E (Composite efficiency indicator): The composite efficiency indicator is the mean of the five subpart efficiency indicators, which gives a broad assessment of the system's performance and ranges between 0.18 and 0.4. This composite indicator indicates that, on average, systems are functioning below their maximum efficiency. The variation in numbers indicates a discrepancy in the overall efficacy of Information Systems Customer Satisfaction Surveys (IS CSS) across various organizations. This composite perspective is a compelling impetus for organizations to undertake thorough evaluations of their security systems, pinpointing precise vulnerabilities and devising improvement plans.

B. Comparative Analysis of Cybersecurity Efficiency Across Industry Leaders

The following compared histograms in Fig. 6. provide a statistical overview of the cybersecurity stances of Facebook, Apple, and Instagram. Each histogram indicates a metric of efficiency, measuring their skills in cyber defense, technological preparedness, and personnel, which are vital for making well-informed strategic cybersecurity choices.

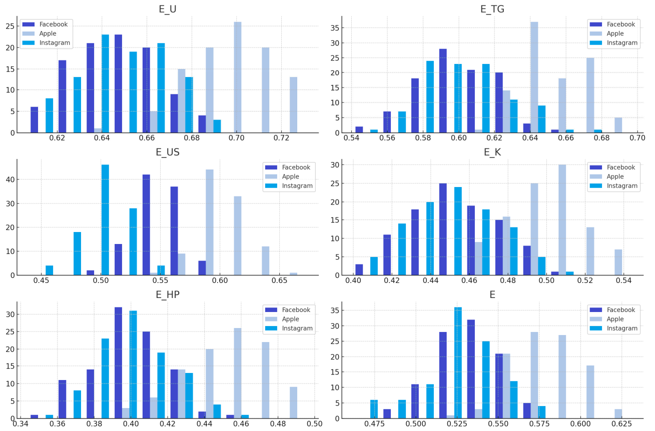


Fig. 6. Comparative Histograms of ISCSS Efficiency Indicators for Facebook, Apple, and Instagram

By combining the numerical data obtained from the histograms with the larger framework of information security and cybersecurity systems, we may deduce various practical consequences:

The **E_U** (Cyber Defense Equipping Coefficient) is Apple's dominant position, shown by a peak at 0.70, indicating that they have a well-equipped cyber defense arsenal and prioritize using advanced technology to protect customer data. The somewhat diminished peaks seen for Facebook and Instagram, approximately at 0.65, indicate a robust, albeit more cautious, allocation of resources towards cybersecurity measures, which distinct business objectives or evaluations of potential risks might impact.

The **E_TG** (Technical Readiness Coefficient) is: The concentration of Apple's values around 0.65 suggests a proactive stance in embracing new security methods and a culture of frequent system upgrades. The values of Facebook and Instagram, around 0.60, are praiseworthy. However, they could suggest a slower pace of embracing new technologies or a distinct standard for implementing system upgrades and maintenance.

E_US (Serviceable Cyber Defense Means Coefficient): The coefficient's central tendency of about 0.60 for Apple indicates a solid and effective lifecycle management of cybersecurity technologies. This is an indication of their dedication to upholding a rigorous operating benchmark. The data indicates that Facebook and Instagram have modal values of about 0.55 and 0.50, respectively. This suggests a need to evaluate and improve their procedures for managing and upgrading cybersecurity resources.

E_K (Staffing Coefficient with IT System Administrators): - A high of about 0.50 for Apple suggests a significant presence of IT administrators, which is crucial for daily operations and strategic cybersecurity efforts. The relatively lesser peaks for Facebook and Instagram indicate that while they have many IT professionals, there may be potential to enhance their teams even more, particularly in domains undergoing rapid technical advancements.

The **E_HP** (Staffing Coefficient with Service Personnel) is a histogram with a central value of 0.45, which suggests that Apple has deliberately invested in support workers. This expenditure will likely improve their capacity to address events and promptly preserve systems' integrity. The peak of about 0.40 on Facebook and Instagram shows a strong staffing level. However, they also suggest the potential advantages of increasing their service people to meet the growing needs of cybersecurity.

The **E** (Composite Efficiency Indicator): Apple's stock reached a high of 0.58, indicating a comprehensive and integrated strategy for cybersecurity based on the composite efficiency indicator. Conversely, the somewhat reduced metrics for Facebook and Instagram indicate the need for these corporations to enhance their concentration on specific facets of their cybersecurity stance to attain a more cohesive and resilient defense system.

C. Practical Applications

The numerical data highlights the need for an adaptable and proactive cybersecurity approach that adapts to changing threats and utilizes the most recent technology breakthroughs. For example, the comparatively lower E_US scores for Facebook and Instagram may motivate these businesses to

Evaluate their cybersecurity asset management and update cycles. Practically, this may include augmenting funding for cybersecurity infrastructure, evaluating the pertinence and efficacy of current capabilities, and adopting a more assertive approach to replacing obsolete technology.

Moreover, the E_K and E_HP indices emphasize the significance of human capital in the field of cybersecurity. More technology must be needed to counter advanced cyber-attacks, highlighting the need for skilled IT system administrators and support workers. Apple's decision to increase employment indicates its recognition that a well-staffed cybersecurity team is not a financial burden but an essential element of the whole value chain. This team plays a direct role in enhancing resilience against cyber-attacks and minimizing system downtime.

The ramifications of these discoveries are substantial. They provide standards for a mature cybersecurity system to industry peers and stakeholders. Academics and practitioners use quantitative data to inform research on cybersecurity investment and staffing strategies. Ultimately, decision-makers may use this information to inform strategic planning, enable efficient resource allocation, and justify investing in complete cybersecurity solutions.

Ultimately, the histograms and their related numerical data provide a comprehensive overview of how prominent firms compare to each other regarding cybersecurity effectiveness. They function as a helpful instrument for comprehending the complex nature of cybersecurity preparedness and the need for a unified strategy that incorporates technology, human resources, and strategic investment. The subtle analysis of these figures helps organizations such as Facebook, Apple, and Instagram make informed choices based on data, improve their security position, and safeguard against the constantly changing realm of cyber dangers.

V. Discussion

The effectiveness of information security and cybersecurity systems (IS CSS) in information and communication systems (ICS) is an essential topic of study, and our work contributes to it by offering a complete and practical approach. Given its comprehensive perspective of efficiency and the simplicity with which it may be applied in regularly used applications such as Microsoft Excel, this technique is different and creative.

The article expands on earlier studies in this area. Maslova presented techniques for analyzing the effectiveness of information system protection systems [13], while Andrieiev proposed a way to evaluate the economic efficiency of the information protection unit [14]. These publications provide essential insights into the many efficiency factors in information security systems. On the other hand, our methodology takes these ideas a step further by providing a more holistic and comprehensive framework for evaluating efficiency, including the equipping coefficient and technical readiness of cyber defense means and the staffing of IT system administrators and service personnel.

Zakharchenko, Korolov [16], Minaiev, Korolev, Zielientsova [17], and Zakharchenko [16] have done substantial work in the field of critical information infrastructure on analyzing the sustainability of critical information infrastructure objects in cyberspace. Their findings emphasize the significance of preserving functioning in cyber-attacks. Our technique supplements existing articles by concentrating on the efficiency of IS CSS, adding another dimension to our knowledge of essential information infrastructure performance.

The work of Kozubtsova, Khlaponin, and Kozubtsov [19-22], [27] and Kozubtsova's dissertation [24] affected the development of our technique substantially. Their study on the effectiveness of cyber security measures, indicators, and quantitative criteria for assessing the effectiveness of IS CSS serves as a solid basis for our work. Our technique expands on these ideas by giving a realistic implementation in Microsoft Excel, making it more accessible to businesses.

By presenting a thorough technique that considers many criteria and can be applied in Microsoft Excel, our study adds new insights to the IS CSS efficiency assessment area. It offers organizations a tangible tool for evaluating and improving there IS CSS and making data-driven choices to improve their information security and cybersecurity. As cyber risks grow, our technique will be vital in maintaining a robust and efficient IS CSS.

VI. Conclusions

Information Security and Cybersecurity Systems in Information and Communication Systems are critical in ensuring information integrity, confidentiality, and availability in today's digital era. The effectiveness of these systems is critical to ensuring that they can successfully fight the ever-changing cyber threats. Our study aimed to contribute to this vital field by presenting a thorough and practical technique for assessing the efficacy of IS CSS.

Our article's methodology incorporates several criteria, including the equipping coefficient of cyber defense means, the technical readiness of cyber defense means, and the staffing levels of IT system administrators and support workers. By considering these factors, our technique provides a comprehensive assessment of the IS CSS's efficiency. This strategy represents a substantial improvement above prior approaches, which often concentrated on particular areas of efficiency.

Another distinguishing feature of our technique is its practical use in Microsoft Excel. This widely available software tool enables simple and efficient computations, making our technique adaptable to various organizations. The simplicity of implementation is intended to encourage the adoption of our technique, assisting organizations to improve their IS CSS.

The paper coincides with the strategic focus on information security and cybersecurity in numerous policy papers and laws. It adds to the substantial body of work done by earlier authors on this subject. Our technique offers a robust and complete framework for assessing the effectiveness of IS CSS by incorporating lessons from various publications.

The findings obtained using our technique give helpful information on the performance of IS CSS. They show the system's strengths and flaws, assisting organizations in finding development opportunities. Organizations may improve their IS CSS and, hence, their resistance to cyber-attacks by exploiting these insights.

The findings illustrate the applicability of our technique. Creating efficiency indicators and associated visualizations demonstrate how our technique may be used in practice. This practical presentation highlights the usefulness of our technique and its potential contribution to IS CSS efficiency assessment.

The article presents a fresh way of assessing the effectiveness of IS CSS. Our approach provides a significant tool for organizations to examine and improve their IS CSS by providing a thorough framework and realistic implementation. As the digital ecosystem evolves and cyber risks increase, our technique will be a valuable resource for sustaining effective and efficient IS CSS. We foresee further development and implementation of our technique in the future, adding to continuing efforts to improve information security and cybersecurity in our increasingly digital world.

References

[1] Y. You, J. Lee, J. Oh, and K. Lee: 'A Review of Cyber Security Controls from An ICS Perspective,' in Editor (Ed.)^(Eds.): 'Book A Review of Cyber Security Controls from An ICS Perspective' (2018, edn.), pp. 1-6

[2] L. Rajesh, & Satyanarayana, P.: "Vulnerability Analysis and Enhancement of Security of Communication Protocol in Industrial Control Systems. ", *HELIX.* , 2019

[3] Y. Hu, Y. Sun, Y. Wang, and Z. Wang: ''An Enhanced Multi-Stage Semantic Attack Against Industrial Control Systems'', *IEEE Access*, 7, 2019, pp. 156871-82

[4] D. Timpson, and E. Moradian: ''A Methodology to Enhance Industrial Control System Security'', *Procedia Computer Science*, 126, 2018, pp. 2117-26

[5] K. Latha, and T. Sheela: "Block based data security and data distribution on multi-cloud environment" *Journal of Ambient Intelligence and Humanized Computing*, 2019

[6] O. I. Yurii Khlaponin, Nameer Hashim Qasim, Hanna Krasovska, Kateryna Krasovska: 'Management Risks of Dependence on Key Employees: Identification of Personnel,' in Editor (Ed.)^(Eds.): 'Book Management Risks of Dependence on Key Employees: Identification of Personnel' (CPITS, 2021, edn.), pp. 295-308

[7] H. Suryotrisongko, and Y. Musashi: 'Review of Cybersecurity Research Topics, Taxono, my and Challenges: Interdisciplinary Perspective,' in Editor (Ed.)(Eds.): 'Book Review of Cybersecurity Research Topics, Taxonomy, and Challenges: Interdisciplinary Perspective' (2019, edn.), pp. 162-67

[8] R. Thomas: ''Total cost of security: a method for managing risks and incentives across the extended enterprise'', 2009

[9] A. H. Petrenko: ''Strategic Defense Bulletin in 2016-2020 (roadmap for Defense Reform). '', *K.: Department of military policy, strategic planning and international cooperation of the Ministry of Defense of Ukraine*, 2016

[10] L. o. Ukraine.: ''On the Basic Principles of Ensuring Cyber Security of Ukraine'', *Bulletin of the Verkhovna Rada (VVR)*, (45), 2017, pp. 403

[11] P. o. Ukraine: ''On Cyber Security Strategy of Ukraine '', 2016

[12] D. o. t. N. S. a. D. C. o. Ukraine: "On State Cyber Security Threats and Urgent Measures to Neutralize Them. "*National Security and Defense Council of Ukraine*, (32), 2017

[13] N. A. Maslova: ''Methods for evaluating the efficiency of information systems protection systems '', *Artificial intelligence*, 4, 2008, pp. 253–64

[14] K. A. Andrieiev: ''Method for assessing the economic efficiency of the information protection unit'', *Information security.*, 5, 2010

[15] L. H. M. Yefimov Y.N.: ''Evaluation of the efficiency of information security measures in conditions of uncertainty'', *Business informatics*, 31, (1), 2015, pp. 51–57

[16] K. I. D. Zakharchenko R.I.: ''Methodology for assessing the sustainability of functioning of critical information infrastructure objects that are functioning in cyberspace'', *knowledge-intensive technologies in space exploration of the Earth*, 10, (2), 2018, pp. 52–61

[17] K. I. D. Minaiev V.A., Zielientsova Y.V., Zakharchenko R.I.: "Critical information infrastructure: assessment of the sustainability of functioning", *Radio industry*, 28, (4), 2018, pp. 59–67.

[18] K. A. V. Minaiev V.A., Korolev I.D., Bondar K.M., Zakharchenko R.I.: "Assessment of the stability of the critical information infrastructure. ", *Bulletin of RosNOU*, 4, 2018, pp. 129–38.

[19] K. Y. I. Kozubtsova L.M., Kozubtsov I.M.: "Methodology for evaluating the efficiency of cyber security measures for critical information infrastructure facilities in organizations. "*Modern information technologies in the field of security and defense*, 41, (2), pp. 17-22

[20] R.-D. I. A. Kozubtsova L. M., Snovyda V.Y.: "Calculation of efficiency indicators for the functioning of the information security and cyber security system'', *Computer integrated technologies: education, science, production.*, 45, 2021, pp. 19-25

[21] C. O. O. Kozubtsov I.M., Kozubtsova L.M., Artemchuk M.V., Neshcheret I.N.: "Selection of individual indicators for assessing the functioning of the information protection system and cyber security of information in information and communication systems of specialized communication", *Cyber security: education, science, technology*, 16, (4), 2022, pp. 19-27

[22] H. O. V. Kozubtsova L.M., Kradynova T.A., Palahuta A.M., Kozubtsov I.M.: "Indicators and mathematical criteria for evaluating the efficiency of the information security system and cyber security of the object of critical information infrastructure", *Scientific and Practical Cyber Security Journal (SPCSJ)*, 6, (1), 2022, pp. 64-71

[23] K. Y. Zabara S., Kozubtsova L.: "Methods for diagnosing cybernetic stability of a special purpose information system. "*Scientific and Practical Cyber Security Journal (SPCSJ)*, 4, (1), 2020, pp. 80–86

[24] L. M. Kozubtsova: ''Improvement of methods for monitoring the cyber stability of a special purpose information system: '', *Open International University of Human Development "Ukraine*," 2020

[25] N. Hashim, A. Mohsim, R. Rafeeq, and V. Pyliavskyi: ''New approach to the construction of multimedia test signals'', *International Journal of Advanced Trends in Computer Science and Engineering*, 8, (6), 2019, pp. 3423-29

[26] N. Qasim, Y. P. Shevchenko, and V. Pyliavskyi: "Analysis of methods to improve the energy efficiency of digital broadcasting", *Telecommunications and Radio Engineering*, 78, (16), 2019

[27] K. L. M. Khlaponin Yu.I., Kozubtsov I.M., Shtonda R.M.: "Functions of the information protection system and cybersecurity of Critical Information Infrastructure", *Cybersecurity Education, Science, Technology*, 3, (15), 2022, pp. 124-34