Methodological Approach to Assessing Information Security of Critical Infrastructure Objects

Yuri Samokhvalov [1], Mykola Brailovskyi [1] and Bohdan Zhuravel [2]

[1] Taras Shevchenko National University of Kyiv, Volodymyrs'ka str. 64/13, Kyiv, 01601, Ukraine
[2] University of York, University Rd., Heslington, York, YO105DD, England

Abstract

Currently, the most common approaches to assessing information security are verification and risk based. However, information security metrics in these approaches are not informative enough, since they consider only the objective aspects of security, completely ignoring the subjective ones. Therefore, they do not allow for the formulation of basic judgments about the level of information security of critical infrastructure objects. In this regard, there is a need to develop a methodological framework for assessing the information security of critical infrastructure objects, considering both objective and subjective aspects of security. The article proposes an approach to assessing information security based on the confidence criterion that the adopted security policy is implemented on a critical infrastructure object. Confidence assessment includes evaluating the trust in the information security of a critical infrastructure object, the quality of the trust assessment model, the background of individuals who conducted such an assessment, and the evaluation of knowledge regarding threats. The generalized desirability function of Harrington is used as a measure of confidence. The proposed approach is relatively simple to implement and can be used as a pilot for developing appropriate methodologies for assessing the information security of both critical infrastructure objects and organizations of various forms of ownership.

Keywords

Information security assessment, assessment, information security, confidence, trust, Harrington function, maturity model.

1. Introduction

Recently, almost all spheres of human activity, society, and the state have become dependent on information, its quality, and relevance. Consequently, there has been a significant increase in cyberattacks on information resources, aiming to obtain crucial information or damage it. Critical infrastructure (CI) objects are most often subjected to these cyberattacks - these are information systems of state bodies, institutions, and companies. A disruption in their operation has a substantial negative impact on the social and economic spheres of the state, its defense capability, and national security [1]. Therefore, issues of information security (IS) are the cornerstone in the operation of such objects. As W. Churchill liked to say, "One has to pay for security, and pay dearly for its absence.

When assessing information security, the following main types of IS metrics are identified: implementation metrics, used to measure the degree to which the security policy is put into practice, and efficiency metrics, used to measure the performance of security services. These metrics form the basis of the most widespread current approaches to assessing information protection: verification-based and risk-oriented. The verification approach is based on comparing the activities and measures to ensure the IS of a CI object with the requirements of standards or guiding documents in the field of information security and protection. As a result, an assessment of the degree of IS compliance with the requirements of the set standards is formed. The risk-oriented approach is associated with risk assessment and management or risk management. It involves considering all possible factors threatening information security, the likelihood of their realization (attacks or incidents), and the value of protected information assets.

Information Technology and Implementation (IT&I-2023), November 20 - 21, 2023, Kyiv, Ukraine
EMAIL: yu1953@ukr.net (A.1); brailovskyim@knu.ua (A.2); bohdan.zhuravel.uk@gmail.com (A.3)
ORCID: 0000-0001-5123-1288 (A.1); 0000-0002-3148-1148 (A.2)

As a result, an assessment of the CI object's ability to effectively manage IS risks achieving its goals will be formed. However, these approaches share a common drawback: they are not informative enough, as they only consider objective aspects of security, completely ignoring the subjective ones. Therefore, they do not allow for a comprehensive assessment of the state of confidentiality, integrity, and availability of information and the overall IS level of the CI object.

In the ISO/IEC TR 15443-1:2005 standard [3], the concept of 'trust' is introduced for the first time as a subjective category of IT security, and methods to ensure trust are provided. These methods can be specific to a particular stage in the lifecycle of a trust object, in accordance with the ISO 9000 series standards, ISO/IEC 15408-1:2009 [4], and the SSE-CMM standard (ISO/IEC 21827:2008) [5]. In work [6], models for assessing trust in information security are proposed, as well as examples of organizing and using measures to ensure assurance and trust. However, the provided examples do not allow for their practical use in assessing IS. In [6], models for assessing assurance in information security are proposed, as well as examples of organizing and using guarantees and trust. Yet, the reviewed examples do not allow for their practical use in evaluating information security. The use of confidentiality as a subjective indicator of an acceptable level of information security is also unquestionable. Moreover, in [7-10], issues of group decision-making based on trust criteria are considered. In [11], an approach to assessing information security is proposed that considers both objective and subjective aspects of security, using measures to ensure assurance and trust. This article is a further development of this approach and addresses issues of accounting for the completeness of information when assessing the information security of critical infrastructure objects.

2. Categories of confidence and trust

From an objective point of view, security can be determined by the state of its object, the presence or absence of certain properties, abilities, etc. From a subjective point of view, security is defined as a certain feeling, perception, awareness, or perception of it by a person. Moreover, it is the subjective interpretation of the concept of "safety" that dominates in everyday consciousness, as evidenced by the results of the study [11]: out of 1506 respondents to the question of how they most often understand "safety" 234 answered - as "calm", 185 - as "confidence" and 128 as "rest."

The safety assessment can be obtained by different methods. However, whatever method is used, such an assessment will be subjective, since the choice of threshold values of security indicators is subjective, expert assessments are subjective, and the assessment of IS risks is subjective. Thus, the object receives the status of "dangerous" or "safe" only because of human evaluative activities, which serves as another confirmation of the need to consider subjective aspects in defining the concept of "safety". The informational security of a critical infrastructure (CI) object, as a state of protection of the informational environment, directly depends on the security of its informational infrastructure. As practice shows, this infrastructure is the primary source of vulnerabilities and IS threats. As new information technologies emerge, so do new vulnerabilities and new attacks. It's evident that mistakes, vulnerabilities, and risks will always exist. Therefore, it's almost impossible to guarantee the security of a CI object's operation. In this situation, we can only assert with a certain degree of confidence that an organization implements (realizes) the adopted security policy. This, in turn, prompts the application of relevant technical and organizational security measures to mitigate vulnerabilities and threats, aiming to ensure a sufficiently acceptable level of trust in the CI object's IS.

It should be noted that the notions "trust" and "confidence" are not identical and are not interchangeable. From the standpoint of psychology, as noted in the standard [6], confidence in the CI object's IS from the point of view of an individual is associated with the belief that he has confidence in its information security, while trust is associated with the proven ability of an organization's information security system to ensure the fulfillment of its security goal. Thus, confidence is an expression of conviction obtained through an assessment of confidence. Trust is determined by the evidence obtained from the assessment of the object. Evidence, usually including an assurance argument, documentation, and other relevant work material, provides the basis for an assurance assertion that is based on the results of the design and security assessment activities.

Confidence is the subject of the individual's perception of the specific safety requirements and the information obtained from the assessment that the assessed item will function in accordance with the specified requirements. Confidence refers to knowledge of the criteria, method, assurance system, and assessment procedures used. At the same time, confidence is based on the knowledge that the dangers we know do not have channels of influence on us, or they are minimized (protection has been undertaken), and we know the capabilities of this protection, or the probability of possible dangers is negligible. Regarding unknown dangers, we have a system that can predict them or to identify them and adequately adapt to them. In addition, the reputation, qualifications, and experience of the assessors are also important factors in building confidence. As a result of individual perception, different people may have different degrees of confidence because of the use of an appropriate method of ensuring confidence, both by the individual and by the organization.

According to [6], it is important to differentiate between trust in accuracy (correctness) and trust in effectiveness. Trust in accuracy is related to the assessment of the compliance of the critical infrastructure object's information security with the requirements of standards or leading global practices in the field of information security and information protection. In contrast, confidence in effectiveness refers to the ability of security functions (processes) to withstand perceived or identified threats. Both correctness assurance and efficiency assurance are important characteristics, and neither is advantageous because both types of assurance operate on significant aspects of the object.

Moreover, in [6] it is noted: "If the security capabilities of an object take into account potential threats and these capabilities have not been analyzed regarding the establishment of accuracy and project implementation, then one cannot be confident in the object's success in countering an attack. Similarly, if an analysis has established the accuracy of the project and the correct implementation of the security capabilities of the object, and the project does not provide for corresponding security functions to counter probable threats, then one cannot be sure that the object will withstand these threats." Therefore, in order to gain overall trust, the object must be assessed for project correctness, implementation, and operation (element of correctness) and must have the appropriate security capabilities to counter identified threats (element of effectiveness)." That is, a combination of these trust measures is needed to gain overall trust in the information security of the critical infrastructure object, which will serve as the basis for our confidence that the organization is implementing the adopted security policy.

3. Model for assessing information security

The most important purpose of an IS assessment of an CI object is to create information needs to improve it IS. In this case, the purpose of the IS assessment is to determine the degree of confidence with which the CI object has implemented the security policy. As noted, confidence in the organization's information security is based on:

- trust in information security, the quality of the trust assessment model and the background of the persons conducting the trust assessment.
- knowledge that known threats do not have channels of influence on business processes or they are minimized (protection has been undertaken) and we know the capabilities of this protection, or the probability of possible threats is negligible.
- knowledge that relatively unknown threats are available that can predict or detecting them.

For clarity, these factors can be represented by the following graph (Fig. 1). Here, the background refers to the reputation, qualifications, and experience of a specialist. Let's introduce the notation:

U is confidence in the IS.
C is credence to IS.
C_k is trust in correctness.
$C_э$ is confidence in efficiency;
P is the quality of the confidence assessment procedures.
P_k is the quality of procedures for assessing confidence in correctness.
$P_э$ is quality of procedures for assessing confidence in efficiency;
B is background of persons conducting trust assessment.
B_k is background of persons conducting the assessment of trust in correctness.
$B_э$ is the background of persons conducting the assessment of the credibility of effectiveness;
Z is knowledge of threats.
R is knowledge of the impact of known threats.

F is knowledge of forecasting and identifying new threats.

Then the formation of confidence in the CI object's information security can be represented as a display

$$\xi\colon\ (C,P,B,Z) \to U, \tag{1}$$

in which objects $C,P,B,Z,$ in turn, are mappings of the form:

$$\xi\colon\ (C_k,C_э) \to C\ \xi_P\colon\ (P_k,P_э) \to P,\ \xi_B\colon\ (B_k,B_э) \to B,\ \xi_Z\colon\ (R,F) \to Z. \tag{2}$$

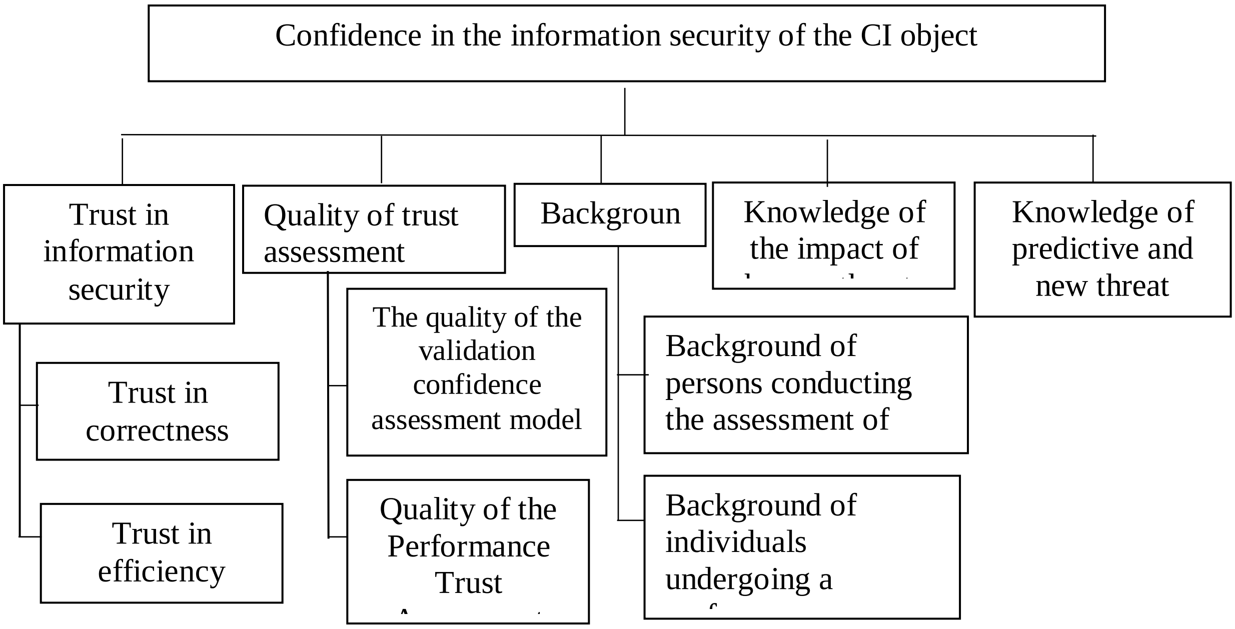
Confidence in the information security of the CI object
Trust in information security
Quality of trust assessment
Backgroun
Knowledge of the impact of
Knowledge of predictive and new threat
Trust in correctness
Trust in efficiency
The quality of the validation confidence assessment model
Quality of the Performance Trust
Background of persons conducting the assessment of
Background of individuals undergoing a

Figure 1: Confidence building factor graph.

If we identify the mapping data with the corresponding tasks, then the assessment of an CI object's information security consists in solving five interrelated and interdependent tasks: assessing confidence in the organization's information security, assessing confidence in information security, measuring the quality of trust assessment procedures, assessing the background of individuals, assessing trust and assessing knowledge regarding the impact known threats and forecasting and identifying new ones. At the same time, the main problem that arises when solving these problems is the choice of the appropriate indicator and the method for calculating it.

One of the basic principles that must be guided when choosing criteria for assessing information security is the unconditional reflection by the criterion of usefulness for the CI object in terms of confidentiality, integrity, and availability of information [12]. Therefore, it is proposed to use confidence as a criterion for assessing information security, since it is an expression of conviction that an CI object's information security system provides these security services, and as an indicator of confidence - the generalized function of Harrington desirability [13]. This allows the use of a single universal psychophysical measurement scale, which establish a correspondence between natural values of indicators in physical scales and psychophysical parameters параметрами subjective linguistic assessments of the "desirability (utility)" of these values for a person. We will use the one-way constrained Harrington desirability function, which is given by:

$$d_i = exp(-exp(-y_i^{н})), \tag{3}$$

where $y_i^{н}$ is the normalized value of the indicator, y_i, d_i is the desirability.

In this case, $y_i^{'}$ the values are calculated by the formula:

$$y_i^{'} = -2 + \frac{7\cdot(y_i - y_{min})}{(y_{max} - y_{min})}, \tag{4}$$

where y_{min} and y_{max} are the lower and upper boundaries of the area of change of the indicator y_i.

After calculating the desirability d_i, they are convolved into a generalized indicator D a generalized desirability function. This function is given by the formula:

$$D = \sqrt[n]{\prod_{i=1}^{n} d_i}. \tag{5}$$

4. Assessment of confidence in the CI object's information security

According to (2), trust in information security C is based on trust C_k in the correct implementation of processes and protective measures and trust $C_э$ in the effectiveness of information security processes.

Assessment of confidence in the correctness of processes and protective measures. Confidence in the correctness of processes and protective measures is reduced to assessing the degree of their compliance with the requirements of the standard, which is taken as the standard ISO/IEC 27000:2009 [1]. This standard (as a family of standards) has been chosen as the base one because, in our opinion, firstly, it absorbed the requirements and recommendations of international standards and best world practices on the field of information security, and secondly, it contains methodological recommendations for assessing information security, which can be applied to organizations of various forms of ownership. If necessary, this standard can be supplemented by national standards in the field of information security, as well as the requirements and recommendations of industry regulatory documents on information security.

To assess the level of IS compliance with the requirements of this standard, group and private IS indicators are used. Group indicators of information security reflect the areas of ensuring the CI object's information security, and private indicators - the requirements of this standard for each of the areas. With the help of private indicators, attributes of the information security processes that are different in nature are assessed, which makes it possible to assess the level of compliance with the requirements of this standard. An integral assessment of the fulfillment of the requirements of the standard [1] is formed from the assessments of the IS group indicators.

Let $O = \{o_i, \middle| i = \overline{1, m}\}$be a set of areas of information security; and $T_i = \{t_{ij} \middle| j = \overline{1, n_i}\}$ be the set of requirements of the standard for the i-th area. We will measure the degree of fulfillment t_{ij} of the requirements using the Harrington scale. As a result, private estimates $d_{ij}$of the correctness (desirability) of the implementation of these requirements will be obtained. Then the group indicator D_i, reflecting the correctness of the implementation of the requirements for the i-th area of information security, is calculated by the formula:

$$D_i = \sqrt[n_i]{\prod_{j=1}^{n_i} d_{ij}}, \tag{6}$$

and the integral estimate by the formula:

$$C_k = \sqrt[m]{\prod_{i=1}^{m} D_i} \tag{7}$$

This assessment reflects the degree of confidence in the correctness of the implementation of processes and protective measures for ensuring the CI object's IS in the requirements of the standard [1]. Assessment of confidence in the effectiveness of information security processes. Confidence in the effectiveness of information security processes is based on the requirements for the composition and maturity model of information technology processes, which are widely used in the field of information security. In [14,15] provides a comparative analysis of the most common and frequently used maturity models, namely:

- Open Information Security Management Maturity Model (O-SIM3).
- Process Capability Model (PCM).
- Business Process Management Maturity Model (BPM MM).
- Community Cyber Security Maturity Model (CCSMM).

The analysis shows that none of the models considered fully reflects all the modern IS requirements for CI objects of various sizes and areas of activity. Therefore, the CI object must be selected and applied to its needs, and, possibly, developed its own maturity model with suitable metrics for it, using the considered models as a template. At the same time, the PCM model in comparison with others, firstly, has a recommendatory rather than descriptive character. Secondly, it is oriented on the IT infrastructure and, thirdly, it is recommended by the standard [2] in the banking sector.

This model will be used as a reference model for the maturity of information security processes. The PCM maturity model is a measure for assessing the completeness, adequacy, and effectiveness of information security management processes. This model defines six levels of maturity from zero to five.

The level of maturity of IS processes is determined by how fully and consistently the organization's management is guided by IS principles, implements IS policies and requirements, uses the accumulated experience and improves information security management system.

We will assess the maturity level of information security processes according to the ISF (Information Security Forum) methodology, which PwC companies widely use to assess the maturity of information security processes in organizations. 21 information security processes are subject to assessment, which are described considering the most well-known international practices and accepted standards (ISO27000, COBIT5 for Information Security, SANS, NIST, etc.) (Table 1). We will assess the level of maturity of IS processes according to the following scale (Table 2).

This scale offers a way to assess "from initial to maximum", by absorbing the requirements of the previous level of maturity by the next. For example, a process meets the second level of maturity only if all the requirements for the first level are met.

Let $PR = \{p_i \mid i = \overline{1,21}\}$be the set of IS processes, and $y_i$be the assessment of the maturity of the i-th process, and $y_i^{н}$is the normalized value $y_i$of the assessment calculated according to (4), where y_{min} =0 and $y_{max} = 5$. Then the particular desirability $d_i$of the process $p_i$is calculated by the formula (3) and the assessment $C_э$of confidence in the effectiveness of the of confidence in the effectiveness of the CI object’s information security processes is calculated by the formula s is calculated by the formula:

$$C_э = \sqrt[21]{\prod_{i=1}^{21} d_i} \tag{8}$$

And finally, the assessment of confidence in the organization's information security is determined by the value of the function:

$$D_C = \sqrt{C_k \cdot C_э} \tag{9}$$

Table 1

Information security processes

№ process	Name of the IB process
1	Information security strategy
2	Management awareness of the importance of information security
3	Risk management IB
4	Compliance management
5	IS audit
6	Information security policy
7	Access control
8	Vulnerability management
9	Management of the life center of the AS
10	Information asset management
11	Change management
12	Information security architecture
13	Communication channel management
14	External communication management
15	Intelligence of information security threats
16	Information security events management
17	Information security incident management
18	Crisis management
19	Ensuring business continuity
20	Raising staff awareness
21	Personnel safety

5. Measuring the quality of the trust and background assessment model

As follows from the above, the assessment of trust is the result of an examination. Therefore, the quality of the trust assessment model in this case depends on the extent to which the expert method and the procedure for its implementation ensure the combination of mathematical models and value judgments of experts to obtain a reliable result. Based on this, quality of model assessment can be represented by a tuple:

$< M, L >$, where M is the expert method, L is the procedure for its implementation. We will evaluate these attributes on the Harrington scale in terms of their usefulness. Let ξ_{M_k},ξ_{L_k} and $\xi_{M_э}$, $\xi_{L_э}$ be estimates of the usefulness of the expert method and the procedure for its implementation, which were used to get $C_k$and $C_э$, accordingly. Then the assessments P_k and $P_э$ quality of models for assessing confidence in correctness and efficiency are calculated by the formulas:

$$P_k = \sqrt{\xi_{M_k} \cdot \xi_{L_k}} \text{ and } P_э = \sqrt{\xi_{M_э} \cdot \xi_{L_э}}, \tag{12}$$

and the quality of the IS trust assessment model according to the formula:

$$D_P = \sqrt{P_k \cdot P_э} \tag{13}$$

Table 2

Scale for assessing the maturity level of information security processes

Level	Maturity level designation	Description
0	Nonexistent	IS process is not running
1	Primitive	The information security process is performed on an irregular basis
2	Elementary	The information security process is carried out on a regular basis and supported at the planning level (including the involvement of stakeholders and the use of relevant standards and guidelines)
3	Formalized	The information security process is carried out, planned, and there are sufficient organizational resources to support and manage
4	Managed	The information security process is carried out, planned, managed and controlled
5	Optimized	The IS process is performed, planned, managed, measured using quantitative indicators (metrics) and is constantly being improved

We will also give an assessment of the background of individuals who have assessed confidence in information security using the Harrington scale. Let ξ_{B_k} and $\xi_{B_э}$ be a desirability of the persons conducting the assessment of trust in correctness and efficiency. Then the background assessment of the persons who assessed the confidence in information security can be obtained by the formula:

$$D_B = \sqrt{\xi_{B_k} \cdot \xi_{B_э}} \tag{14}$$

It should be noted that to obtain more accurate assessments of the quality of the trust computation model for information security and the background of those conducting such calculations, a group expert evaluation is required. In this context, the approach discussed in [16] can be used to reconcile expert assessments.

6. Assessment of knowledge regarding threats

Knowledge of threats (Z) can be characterized by the completeness and reliability of information (evidence) that, firstly, known threats do not have channels of influence on IS object or they are minimized (protection has been undertaken) and we know the capabilities of this protection, or is negligible the probability of possible threats (R). And second, that there are means capable of predicting or detecting new threats (F).

Evaluation of information completeness. The completeness of information relates to the main informational dialectical contradiction between the need for complete knowledge about threats and the lack of this knowledge. In socio-technical systems, the completeness of information is an indicator $\eta \in [0,1)$ characterizing the measure of its sufficiency for deciding. This is a very uncertain and relative indicator since the completeness of information is evaluated solely in relation to a specific task. Given the above, we will assess the completeness of the initial data by filtering by comparing the available information and the “reference”, which is sufficient to assess knowledge about threats. Such information, in accordance with DSTU 3396.0-96 [17], will be represented by the corresponding morphological threat tree (Fig. 2).

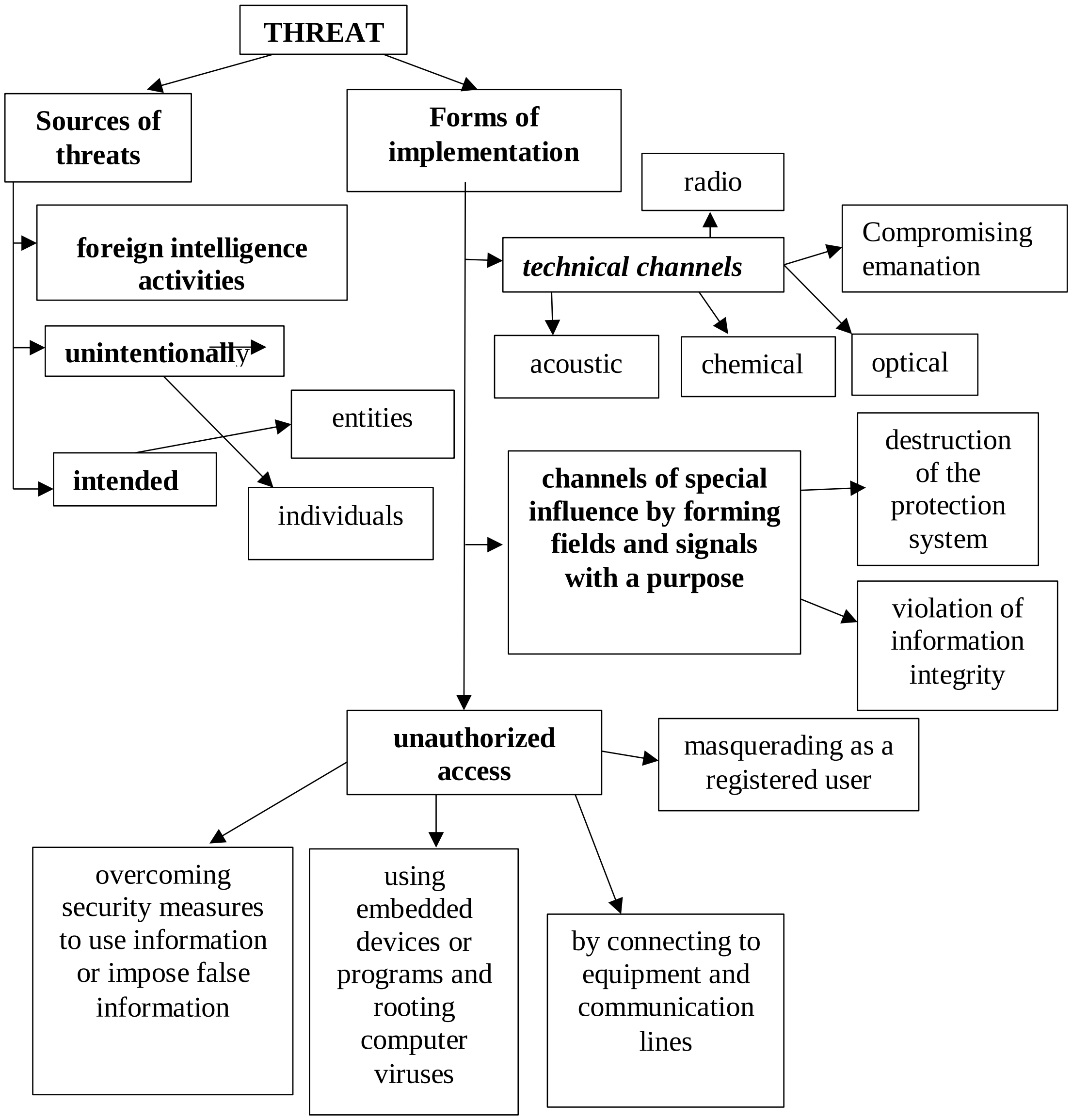
THREAT
Sources of threats
Forms of implementation
foreign intelligence activities
unintentionally
intended
entities
individuals
radio
technical channels
Compromising emanation
acoustic
chemical
optical
channels of special influence by forming fields and signals with a purpose
destruction of the protection system
violation of information integrity
unauthorized access
masquerading as a registered user
overcoming security measures to use information or impose false information
using embedded devices or programs and rooting computer viruses
by connecting to equipment and communication lines

Figure 2: Morphological tree of threats.

This tree consists of elementary structures (Fig. 3), which define the morphology of the corresponding information headings (H) with the required level of detail (h_i). Each detail, in turn, is a parent rubric.

For example, the heading Sources has a detail of the activities of foreign intelligence services, not intentional and intentional. In turn, detailing not intentional and intentional are headings with detailing individuals and legal entities. Then the headings (subheadings) of this tree are assigned the weights of their influence (importance) on the top-level elements. Further, the available information is compared with the morphological tree by assigning a Boolean parameter to α_i its elements: $\alpha_i = 1$ if the i-th rubric (subcategory) is present in the source data and $\alpha_i = 0$ otherwise. Then, similarly to the procedure for synthesizing global priorities of the method of analysis of hierarchies, the convolution of the obtained estimates of the elements of the morphological tree is carried out. As a result, an estimate of the completeness of the initial information will be obtained.

Let the elements of the structure (Fig. 3) have the following parameters: $H = (\mu, \alpha)$, $h_i = \{(\mu_i, \alpha_i) | i = \overline{1, n}\}$, where μ, α and μ_i, α_i are the weight coefficients and. Boolean values of the elements H and h_i, respectively. Then the result of the convolution of the estimates of this structure is the value that is taken $a^* = \sum_{i=1}^{n} \mu_i \cdot \alpha_i$ as a parameter of α its parent element H. This parameter, in fact, expresses the degree of informational completeness of the corresponding heading, considering the importance of its subheadings, and, as a result, is taken as an assessment ξ_Q of the completeness of the original information. *Assessment of the reliability of information.* Under the reliability of information, we mean its property to reflect the objective reality with the necessary accuracy. The criterion for reliable information is the absence of distorted or false data, and the probability of its truth is used as a measure of quantitative assessment. When assessing the reliability of information according to, we will use the Kent scheme [18], which gives a clear classification of information in terms of the degree of its reliability (Table 3).

Table 3
Kent scheme

RELIABILITY					
Odds behind			Odds against	Degree of confidence expressed in odds	Degree of confidence expressed in terms of probability
Confidence level	99 85	▩	1 15	Almost definitely, the information is reliable (odds: for - 9, against - 1)	Almost definitely, the information is reliable (almost certainly yes)
	84 60	▧	16 40	There are many chances that the information is reliable (odds: for - 3, against - 1)	Probably the information is reliable (probably yes)
	59 40	▦	41 60	The odds are approximately equal (odds: for - 1, against - 1)	
	39 15	▥	61 85	There are many chances that the information is unreliable (odds: for - 1, against - 3)	Probably the information is unreliable (probably not)
	14 1	▨	86 99	Almost definitely, the information is unreliable (odds: for - 1, against - 9)	Almost certainly the information is unreliable (almost certainly not)
UNRELIABILITY					

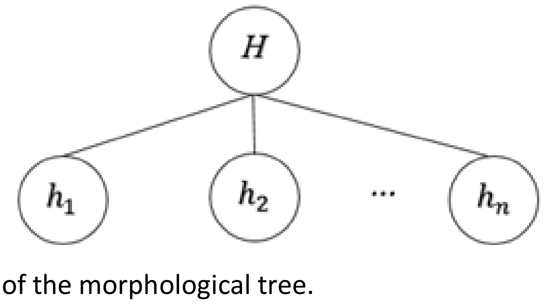

Figure 3: Elementary structure of the morphological tree.

Then, knowing the reliability of the information available regarding threats and its completeness, using the Harrington scale, it is possible to determine the usefulness of this knowledge as a factor in ensuring confidence. Let ξ_R, ξ_F be assessments of the reliability of evidence of knowledge R and F also ξ_Q is an assessment of information's density. Then estimates d_R, d_F, d_Q can be obtained using formulas (3) and (4). Then the assessment of the usefulness of knowledge is calculated by the formula:

$$D_Z = \sqrt[3]{d_R \cdot d_F \cdot d_Q} \tag{15}$$

Finally, the degree $D_U$of confidence with which an CI object has implemented a security policy is determined by the value of the function:

$$D_U = \sqrt[4]{D_C \cdot D_P \cdot D_B \cdot D_Z} \tag{16}$$

7. Practical implementation

Consider an example that illustrates the proposed approach to assessing an CI object's information security. To ensure a comprehensive analysis and objectivity of assessments, it is advisable to involve heads of information security services in CI object as experts [19]. A. Assessment of confidence in the CI object's information security. As noted, trust in information security is based on trust in the correct implementation of processes and protective measures and trust in the effectiveness of information security processes. The assessment of confidence in the correctness (correctness) of processes and protective measures will be given using group and private indicators of information security. The corresponding areas of information security (Table 4) are used as group indicators.

Tables 4

Areas of information security

№	Areas of information security
1	Provision of information security in the appointment and distribution of roles and ensuring confidence in personnel;
2	IS provision at the stages of the CI object's IS life cycle;
3	Providing information security when managing access and registration;
4	Providing IS with anti-virus protection means;
5	Providing information security when using Internet resources;
6	Providing information security when using cryptographic information protection tools;
7	Provision of IS for technological processes;
8	Providing IS information technological processes;
9	Processing personal data in the CI object;
10	IS provision of technological processes within the framework of which personal data is processed.

Table 5

Estimates of private indicators using anti-virus protection tools

Indicator number	Private indicators information security	Private indicator evaluation d_{1j}
1	Antivirus protection	0,83
2	Are anti-virus protection tools used on all automated workstations and IS servers of the CI object, unless otherwise provided by the technological process?	0,68
3	Has the organization defined, implemented, recorded and monitored procedures for installing and regularly updating anti-virus protection tools (versions and databases) on workstations and object's servers?	0,95
4	Is the functioning of the constant anti-virus protection in automatic mode and the automatic installation of updates for the anti-virus software and its databases organized?	0,7
Assessment of a group indicator D_1		0,78

For each area of information security assurance, there is a corresponding list of specific evaluation indicators. To reduce the volume of the article, we will consider, for example, only the 4th and 6th areas of information security and the first 4 private indicators that correspond to these areas. The assessment of indicators is carried out according to a methodology that includes questionnaires using the Harrington scale, and group indicators are calculated using the formula (6). The corresponding estimates are given in Tables 5 and 6.

As a result, the assessment of confidence in the correctness (correctness) of processes and protective measures according to (7) is equal to:

$$C_K = \sqrt{D_1 \cdot D_2} = \sqrt{0,78 \cdot 0,85} = 0,81.$$

Assessment of confidence in the effectiveness of information security processes. Such an assessment is carried out for all processes presented in Table 3 on a scale (Table 4). The following evidence should be used for analysis [10]:

- documentary evidence of the assessment of potential losses (damage) to the CI object's business because of the impact (possible implementation) of information security threats.
- documentary evidence of the choice of the risk minimization (treatment) option in relation to all risks assessed after the process has been completed.
- documentary evidence of a decrease in the number of potential incidents caused by risks and identified ex post facto.
- documentary evidence of an increase in the number of identified risks, the impact of which has been weakened.

Table 6

Estimates of private indicators information security using cryptographic information protection tools

Indicator number	Private indicators of information security when using cryptographic	Private indicator evaluation d_{2j}
1	Is the cryptographic means of information protection applied at the critical infrastructure facility in accordance with the information security threat model and the intruder model adopted by the organization?	0,87
2	Do cryptographic protection tools used to protect personal data have a class not lower than KC2?	0,92
3	Is the work to ensure information security using cryptographic information protection tools carried out in accordance with current legislation, regulations governing the operation of cryptographic information protection tools, technical documentation for cryptographic information protection tools and licensing requirements?	0,74
4	Has a specific policy regarding the use of cryptographic means of information protection at the critical infrastructure facility been approved?	0,88
Assessment of a group indicator D_2		0,85

The evaluation results are shown in Table. 7, in which the values, y_i, $y_i^н$ and d_i are obtained, respectively, using the Harrington scale and formulas (8) and (9).

As a result, the assessment $C_э$ of confidence in the effectiveness of the CI object's information security processes in accordance with formula (10) is equal to:

$$C_Э = \sqrt[21]{\prod_{i=1}^{21} d_i} = \sqrt[21]{0{,}282} = 0{,}942\ .$$

Thus, the assessment of confidence in the CI object's information security is determined by the value of the function (11):

$$D_C = \sqrt{0{,}81 \cdot 0{,}942} = 0{,}874$$

B. Measuring the quality of the trust and background assessment model. According to clause 6. The quality of the trust assessment model will be assessed from the point of view of the extent to which the expert method and the procedure for its implementation ensure the combination of mathematical models and value judgments of experts to obtain a reliable result. In this case, we will use the Harrington scale. Let $\xi_{M_k} = 0.85$, $\xi_{L_k} = 0.93$ and $\xi_{M_э} = 0.95$, $\xi_{L_э} = 0.93$ be estimates of the usefulness of the expert method and the procedure for its implementation for obtaining reliable estimates of confidence C_k and $C_э$, accordingly. Then, using formulas (12) and (13), we obtain the following estimates:

$$P_k = \sqrt{0.85 \cdot 0.93} = 0.89, P_э = \sqrt{0.95 \cdot 0.93} = 0.94, D_P = \sqrt{0.89 \cdot 0.94} = 0.91.$$

We will also give an assessment of the background of individuals who have assessed confidence in information security using the Harrington scale.

Let $\xi_{B_k} = 0.76$ and $\xi_{B_э} = 0.83$ be the assessments of the background of the persons who assessed the trust in correctness and efficiency. Then according to (14) we get:

$$D_B = \sqrt{0.76 \cdot 0.83} = 0.79.$$

Table 7

Assessments of confidence in the effectiveness of information security processes

№ domain	Name of the IS process	y_i	$y_i^{\text{н}}$	d_i
1	Information security strategy	4	3,6	0,973
2	Management awareness of the importance of information security	3	2,2	0,895
3	Information security risk management	4	3,6	0,973
4	Compliance management	4	3,6	0,973
5	IS audit	3	2,2	0,895
6	Information security policy	5	5,0	0,993
7	Access control	4	3,6	0,973
8	Vulnerability management	3	2,2	0,895
9	Management of the life center of the AS	4	3,6	0,973
10	Information asset management	3	2,2	0,895
11	Change management	3	2,2	0,895
12	Information security architecture	4	3,6	0,973
13	Communication channel management	4	3,6	0,973
14	External communication management	3	2,2	0,895
15	Intelligence of information security threats	3	2,2	0,895
16	Information security events management	4	3,6	0,973
17	Information security incident management	4	3,6	0,973
18	Crisis management	3	2,2	0,895
19	Ensuring business continuity	5	5,0	0,993
20	Raising staff awareness	3	2,2	0,895
21	Personnel safety	5	5,0	0,993

C. Assessment of knowledge regarding threats. Let $\xi_R = 81$ and $\xi_F = 90$ be estimates of the reliability of evidence of knowledge R and F according to the Kent scale, ξ_Q=0.85 is the degree of completeness of the available information. Assuming for confidence estimates in (4) $y_{min} = 1$ and $y_{max} = 99$ we get: $y_R^{н} = 3{,}71$, $y_F^{н} = 4{,}92$ and to estimate the degree of completeness, assuming $y_{min} = 0$ and $y_{max} = 1$, we get $y_Q^i = 3.95$. Then desirability d_R, d_F and d_Q according to (3), will have the following values: $d_R = 0{,}98$, $d_F = 0{,}99$, $d_Q = 0{,}98$. And finally, using formula (15), we obtain an estimate of the usefulness of knowledge regarding threats:

$$D_Z = \sqrt[3]{d_R \cdot d_F \cdot d_Q} = \sqrt[3]{0{,}98 \cdot 0{,}99 \cdot 0.98} = 0.98,$$

and according to formula (16) the degree of confidence with which the CI object has implemented the security policy:

$$D_U = \sqrt[4]{D_C \cdot D_P \cdot D_B \cdot D_Z} = \sqrt[4]{0{,}87 \cdot 0{,}91 \cdot 0{,}79 \cdot 0{,}98} = 0{,}88$$

Such confidence on the Harrington scale can be interpreted as “very high”.

8. Conclusion

A methodical approach to assessing the information security of an CI object by the criterion of confidence is proposed. The factors of confidence formation are considered, and the generalized Harrington function is proposed as its integral indicator. The assurance assessment includes an assessment of the CI object’s information security assurance, the quality of the assurance assessment model, the background of the individuals who conducted the assessment, and the threat knowledge assessment. In general, the considered approach can be used as a pilot for the development of appropriate methods for assessing the information security of CI objects of various forms of ownership, and the considered example clearly demonstrates its availability.

9. References

[1] Law of Ukraine "On Critical Infrastructure" No. 1882-IX, 2021

[2] ISO/IEC 27000:2009, Information security management systems - Overview and vocabulary (Information security management system. General overview and terminology). [Electronic resource]. – URL https://www.iso.org/standard/41933.html.

[3] ISO/IEC TR 15443-1:2005 «Information technology – Security techniques – A framework for IT security assurance. Part 1: Overview and framework». [Electronic resource]. – URL https://www.iso.org/standard/39733.html

[4] ISO/IEC 15408-1:2009 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model [Electronic resource]. – URL https://www.iso.org/standard/50341.html

[5] ISO/IEC 21827:2008 Information technology -- Security techniques -- Systems Security Engineering -- Capability Maturity Model® (SSE-CMM®) [Electronic resource]. – URL https://www.iso.org/standard/44716.html

[6] Imamverdiev Ya.N. Model for assessing confidence in the information security of an e-state // Problems of information technologies. Institute of Information Technologies of ANAS, Baku, Azerbaijan. 2015, No. 1, pp.25-32.

[7] Samokhvalov Yu.Y. Developing the Analytic Hierarchy Process Under Collective Decision-Making Based on Aggregated Matrices of Pairwise Comparisons. Cybern Syst Anal 58, 758–763 (2022). https://doi.org/10.1007/s10559-022-00509-3

[8] W. Wu, G. Kou, and Y. Peng, "Group decision-making using improved multi-criteria decision making methods for credit risk analysis," Filomat, Vol. 30, Iss. 15, 4135–4150 (2016). https://doi.org/10.2298/FIL1615135W.

[9] K. Peniwati, "Group decision making: Drawing out and reconciling differences," Int. J. Anal. Hierarchy Process, Vol. 9, No. 3, 385–389 (2017). https://doi.org/10.13033/ijahp.v9i3.533.

[10] E. Forman and K. Peniwati, "Aggregating individual judgments and priorities with the analytic hierarchy process," Eur. J. Oper. Res., Vol. 108, Iss. 1, 165–169 (1998). https://doi.org/10.1016/s0377-2217(97)00244-0.

[11] Samokhvalov Yu.Y., Brailovskyi M.M. Assessment of organization's information security on the criterion of confidence. Ukrainian Information Security Research Journal. 2019. Vol. 21, no. 1. URL: https://doi.org/10.18372/2410-7840.21.13445

[12] Canadian Tusted Computer Product Evaluation Criteria, v. 3.0. Canadian System Security Centre, Communications Security Establishment, Government of Canada, 1993.

[13] Harrington, E.C. The desirable function. Industrial Quality Control. – 1965. –Vol. 21. No. 10. – pp. 494–498.

[14] [11] Cobit 5: a model for evaluating processes [Electronic resource]. - URL: https://cleverics.ru/subject-field/articles/554-cobit5-pam

[15] Smirnov, I., Kutyrev, A., Kiktev, N. (2021). Neural network for identifying apple fruits on the crown of a tree. *E3S Web of Conferences. International scientific forum on computer and energy Sciences, WFCES 2021,* 01021. https://doi.org/10.1051/e3sconf/202127001021

[16] Samokhvalov, Yu.Ya. Matching of expert estimates in preference relation matrices (2002) Upravlyayushchie Sistemy i Mashiny, (6), pp. 49-54

[17] DSTU 3396.0-96 [Electronic resource]. – URL https://tzi.com.ua/downloads/DSTU%203396.0-96.pdf

[18] Kent S. Strategic Intelligence for American World Policy. Princeton: Princeton University Press. – 1949. – 226p.

[19] Babenko, T., Hnatiienko, H., Ignisca, V., Iavich, M. Modeling of critical nodes in complex poorly structured organizational systems. Proceedings of the 26th International Conference on Information Society and University Studies (IVUS 2021), Kaunas, Lithuania, April 23, 2021 / CEUR Workshop Proceedings, 2021, 2915, pp. 92–101.