Base of Models of the Information Security Risks Assessment System

Yurii Khlaponin, Olga Izmailova
Kyiv National University of Construction and Architecture
Kyiv, Ukraine
y.khlaponin@knuba.edu.ua,
izmailova.ov@knuba.edu.ua

Hanna Krasovska, Kateryna Krasovska
Taras Shevchenko National University of Kyiv
Kyiv, Ukraine
hanna.krasovska@knu.ua,
katerina.krasovska@knu.ua

Nataliia Bodnar
Al-Rafidain University College
Baghdad, Iraq
natalia.bodnar@ruc.edu.iq

Saad Qasim Abbas
Al-Turath University College
Baghdad, Iraq
saad.qasim@turath.edu.iq

***Abstract*—Background: New technologies, global computerization, and cloud computing provide new risks to modern enterprises' information environments. It takes an effective information security risk management system to balance user data accessibility with data security.**

Objective: The aim is to investigate the development of a human-machine information technology for risk assessment, which is critical to a company's information security risk management system. Despite the real-world obstacles of risk assessment decision-making, the emphasis is on assuring systematic risk assessment and the dependability of the implementation process.

Methods: The study employs current risk management methodology, decision support systems, and expert assessment methods. It also looks at worldwide standardization initiatives, existing risk management systems, procedures, and the responsibilities of expert evaluations. Furthermore, numerous techniques, models, and methodologies of individual risk assessment components are examined.

Results: The study emphasizes the dominating importance of the "human factor" in risk management systems, particularly the issues associated with the complexity of analysis and the need for large resources. Tools that improve the systematization, formalization, and standardization of assessment procedures are required. To enhance risk management, the study underlines the need of shifting to information technology based on current decision support systems.

Conclusion: This article adds to our knowledge of how to use information technology for risk assessment inside a risk management system. Integrating systemically integrated model bases and exploiting the capabilities of current decision support systems may give a more efficient, systematic, and dependable way to addressing information security threats.

Keywords: Information security risk assessment, decision support system, model base, knowledge base, information asset, information asset vulnerability, expected levels of damage, multi-criteria approach, expert evaluation.

I. Introduction

New information technologies, the constant expansion of the scope of their use, global computerization and the use of information and computing networks, cloud computing have created new sources of threats to the entire information environment in which a modern company operates. In these conditions, the issue of building and improving the information security risk management system is relevant at various management levels of the company.

The main task of a company's risk management system is to find and optimize a compromise between two priority needs: transparency and accessibility of data for users, on the one hand, and guaranteeing data security and a reliable level of information and cyber security on the other. The role and significance of the risk management system for the successful implementation of this task is confirmed by the active work of international standardization organizations in this area, the development and accumulation of universal effective risk management systems in the practice of modern companies [1-6]. The dominant role in these systems is played by the "human factor" associated with obtaining basic information through workshops, interviews, questionnaires and decision-making based on qualitative and quantitative indicators established on the basis of expert assessment. The accumulated experience of their wide application determined their high efficiency and allowed us to focus on the existing problems: complexity and significant time spent on the implementation of analysis and management processes, the need to attract significant resources for use within the organization or from the outside, insufficient level of validity of the decisions made. This allows us to draw a conclusion about the relevance of further development of the capabilities of risk management systems based on the development and improvement of human-machine tools for the implementation of the stages of risk management in the concept of implementation of the approaches of the specified systems. This toolkit should be aimed at increasing the level of systematization, formalization, standardization of assessment processes, the flexibility of linking implementation options to existing decision-making situational conditions, which requires the creation, application and development of interactive information technology for decision-making in the risk management system.

II. Analysis of literature sources and statement of the problem

The activity of international standardization organizations confirms the importance of information security issues and the relevance of continuous improvement of information security risk management models, methods and mechanisms. At the main approach to ensuring information security is a risk-based protection strategy (Risk-Based Protection Strategy), which provides for the construction of an information security system that is integrated into the organizational and technical infrastructure of the company. In the modern theory and practice of building risk management systems, there is a sufficient number of highly recommended and quite widely used methodologies, techniques and risk management methods, which include NIST 800-30 [1;2 p.10-11], CRAMM [2 p. 11-14; 3], OCTAVE [2 p. 11-14; 4, 5], Allegro, MEHARY [2, page 17; 6], Magerit [2, page 19; 7]. Their common feature is a single three-level approach to risk management: "organization - business processes - information systems" and orientation towards solving a poorly structured risk assessment problem in conditions of incomplete data certainty and weak formalization of assessment procedures. The analysis of the stages of risk management made it possible to determine that the basis for determining the order of development and evaluating the effectiveness of the implementation of security measures is such a functional component as risk assessment, which is separated in this article as an object of further research.

One of the most popular and widely used developments in the risk management system is the National Institute of Standards and Technology (NIST) risk assessment methodology. It involves forecasting two parameters: potential damage and the probability of threat realization on a qualitative scale without its quantitative interpretation. At the same time, the value of each variable, in particular risk, is evaluated on a three-level scale. There is proposed a "rigid" mechanism for obtaining risk assessments that significantly limits the accuracy of the results, ensuring their efficiency and reproducibility. In more complex methods, such as OCTAVE [2,4-5], Allegro [2,6], MEHARY [2,6], Magerit [2,7], the influence of information resource relationships is taken into account, and when forming protection measures, database of possible threats. The peculiarity of these works is that the risk assessment is carried out on the basis of a single generalizing indicator. Thus, in the OCTAVE method, the risk value is defined as the average value of the company's annual losses as a result of information threats. The CRAMM methodology [2,3] is based on a comprehensive approach to risk assessment that combines quantitative and qualitative methods of analysis. The methodology is universal and suitable for both large and small organizations, both in the public and commercial sectors. CRAMM includes a toolkit for assessing "pure" risks, regardless of the control mechanisms implemented in the system. At the stage of risk assessment, it is assumed that countermeasures are not applied at all, and a set of recommended countermeasures to minimize risks is formed from this assumption.

Approaches, models and methods of individual components of risk assessment were analyzed: identification of AI, threats, vulnerabilities, potential losses from threat implementation. Thus, it provides wide opportunities for vulnerability assessment Common Vulnerability Scoring System (CVSS) is an open standard used to calculate quantitative assessments of vulnerabilities of the system as a whole and its individual assets [7]. CVSS offers a convenient toolkit for calculating a numerical indicator on a ten-point scale, which allows security professionals to more quickly make decisions about how to respond to a particular vulnerability. Considerable attention of researchers is devoted to improving the reliability of the estimate of expected losses when the threat is realized. In many of them, the tendency is noted that the evaluation of potential losses from the realization of the threat should, as a rule, depart from the standard of taking into account only financial losses, and requires improvement of the evaluation results based on the structuring of loss estimates according to many criteria [8-13]. In [14], experimental studies of ways to improve the multi-criteria approach to evaluation were carried out. It is based on an expert assessment of losses based on the method of direct assessment and the method of analyzing hierarchies, structuring different levels of the consequences of the threat of expected losses and considering them as probabilistic values. Various levels of the hierarchy of criteria and the weight of their influence on the calculation results are taken into account.

The conducted research allowed the authors to conclude the need to base the assessment of information security risks on the generated scientific ideas, accumulated experience and practical recommendations of many domestic and foreign scientists and researchers in the field of risk analysis. In modern conditions, risk management is increasingly moving away from strict the target setting of their avoidance and minimization and is aimed at the formation of compromise options for decisions - the possibility of accepting a certain level of risk and using it for the benefit of the company. Based on the analysis of literary sources, it is possible to conclude that the following are currently the real methods of assessing the risks of information systems:

- accumulation and statistical processing of data in the implementation of various types of threats;
- creation and accumulation of statistical data during natural experiments;
- statistical and simulation modeling;
- expert assessment.

Determining the importance and effectiveness in the relevant situational conditions of the use of the first three methods, today the main standards and achievements are based on the application of expert evaluation methods. The expert evaluation method provides an organizational and logical-mathematic evaluation toolkit that corresponds to the real conditions of weak structuring of the evaluation problem. The method is related to establishing and combining the knowledge of the most competent persons in the field of information security. Currently, a number of various methods and models are used, aimed at determining the components of the mathematical apparatus of risk assessment in conditions of incomplete data certainty based on expert assessment methods [13-17].The analysis of modern research directions shows that the issue of further improvement of the toolkit of assessment by account is urgent creation of a universal human-machine information technology for risk assessment, the formalized description of which minimizes the possibility of errors in the implementation of assessment processes. It was concluded that a significant lever for increasing the effectiveness of risk management in real conditions of weak structuring of management processes and conceptual uncertainty will be the transition to the use of information technology based on the capabilities and advantages of modern decision support systems (DSS). From the point of view of the system approach, when creating the DSS, it is necessary to determine the principles and requirements for the system, which takes into account the use of significant levers for improving the evaluation efficiency.

The purpose of the authors' research is to find and analyze ways to solve the compromise problem, which requires, on the one hand, to ensure the systematic evaluation taking into account the multifaceted requirements for the degree of formalization of processes and improvement of the mathematical apparatus of implementation, increasing the level of reliability and accessibility of implementation, and, on the other hand, taking into account the inconsistency of the real conditions of an unstructured decision-making problem and conceptual uncertainty. An attempt to contribute to a partial solution of this problem is implemented in this study.

The purpose of the article is to analyze the approach to the implementation of the information technology of risk assessment in the risk management system based on a systemically linked base of models with the use of modern capabilities of the DSS. To achieve the goal, the following tasks were set:

- Define the base of information technology models;
- Conduct research on basic models and methods of their implementation.

The article is well-structured to aid readers in understanding approaches for assessing information security risks. The opening portion situates the subject within the larger field of information security, emphasising its importance and providing the groundwork for the following topics. After presenting the suggested model, the paper continues conducting a thorough Literature Review, which involves analysing previous models and theoretical frameworks in detail. The article aims to propose a fresh paradigm, including an investigation of its philosophical foundations, evolutionary path, and practical applications. The following part is a thorough Analysis and Discussion, where we extensively review the model and its consequences. The article's conclusion section presents a succinct overview of the main arguments and suggests possible directions for further academic exploration in this field.

III. Background

The construction of information technology risk assessment (ITRA), which is developed as a human-machine risk assessment tool based on such concepts as asset, vulnerability, threat and losses at the level of information assets, is proposed to be based on the principles corresponding to the possibilities of building modern DSS:

1) ITRA should ensure the system consistency of the formalization apparatus, mathematical support and rules for obtaining information from the decision-maker (DM) and experts. The opinion of specialists and the information generated and processed in ITRA should represent a single entity for decision-making.
2) ITRA should provide at each stage of technology a convenient interface for a specialist to work with databases and knowledge for a specialist to work conveniently with documentation, minutes of meetings, standards, rating scales, catalogs of assets, threats and vulnerabilities.
3) ITRA must ensure that the existing situational conditions of decision-making are taken into account during the assessment processes and be oriented to the flexible generation of alternative assessment scenarios.
4) ITRA must ensure that each evaluation scenario is formed based on the established base of models.
5) The formation of the ITRA model base takes into account the following basic provisions:

- The company operates a fixed set of information systems (IS).$i \in I, i = \{1,2,\dots,k^*\}$
- The information asset (IA) of the company is defined as the object of ensuring information security considered as a set of information) that represents value for the organization and (or) its customers, business partners and employees. Each IS having a set of information assets:

$$A_i = \left\{a_1^i, a_2^i, \dots, a_s^i, \dots, a_{s_i'}^i\right\}, i \in I, s \in s'$$

- For each IS, a finite set of possible threats is known for a certain time:

$$i \in IZ_i = \left\{z_1^i, z_2^i, \dots, z_l^i, \dots, z_{l_i'}^i\right\}, i \in I, l \in l'$$

- It is determined: $E_i^p = \{e_1^i, e_p^i, \dots, e_{p^*}^i\} p \in P = \{1,2,\dots,p^*\}$ - a set of experts participating in the assessment. For each expert, an indicator of his competence can be set, which can be taken into account when forming a group of experts, as well as when calculating generalized assessments of a group of experts. θ_p
- It is possible to implement various risk assessment scenarios. Each scenario should reflect the decision-making conditions chosen by the user from the set of possible alternatives provided to him.
- In order to carry out an assessment of losses during the realization of threats to information assets for the comprehensive assessment scenario, a basic set of loss assessment criteria is established:

$$F = \{f_1, \dots, f_j, \dots, f_{j^*}\} = \{f_j, j \in J\}, J = \{1,2, \dots, j^*\}$$

Examples of criteria are: "financial damage", "reputational damage", "possibility of functioning of the information system", etc. The set of criteria by which the assessment is carried out may differ depending on the information system, the information asset and the threat under consideration .f_j. During the evaluation of the DM and experts, it is possible to make corrections in the composition of the selected set. Installed plural basic indicators for qualities inherent in vulnerability

$$V = \{v, \dots, v_y, \dots, v_{y'}\} = \{v_y, y \in Y\}, y = \{1,2, \dots, y'\}$$

For example, basic indicators of the general CVSS vulnerability assessment system [7]:

- the value of the "access vector" metric, the value of the "access complexity" metric, the value of the "authentication" metric, the impact on privacy, the impact on integrity, the impact on availability:

$$V = \{v, \dots, v_y, \dots, v_{y'}\} = \{v_y, y \in Y\}$$

During the evaluation of the DM and experts are given the opportunity to make corrections in the composition of the selected set.$y = \{1,2, \dots, y'\}$.

- Availability and presentation in the knowledge base of catalogs of threats, violators, vulnerabilities, types of losses and their evaluation criteria, qualitative and quantitative scales of measurement of various objects of expert evaluation.

The informational basis of work with risk assessment technology TAR_{isl} (f.1) and the generalized mathematical model of risk assessment AR_{isl} (f.2) is proposed to be characterized by the following ratios:

$$TAR_{isl} = \{ \ (\overline{R_{\imath sl}};\ \overline{V_{\imath sly}; P_{\imath sly}}) | i \in I, s = \overline{1, s'};\ l = \overline{1, l'};, y = \overline{1, Y})\} \tag{1}$$

$$AR_{isl} = \ R_{isl} \times \sum_{y=1}^{Y} V_{isly} \times P_{isly}; \tag{2}$$

$\overline{R_{\imath sl}}$– probability (frequency)implementation of the lth threat to the sth asset;

${V_{isly}}_{ij}$– expected vulnerabilityof the s-th asset when the l-th threat is realized based on the y-th indicator qualities inherent in vulnerability, [0 ÷ 1];

P_{isly}- multifactorial expected costs upon realization of the lth threat to the s-th asset, taking into account the y-th qualities inherent in vulnerability.

1. Expert evaluation methods are widely used as a basis for building the model base. In order to improve the results of expert evaluation by increasing their reliability, on the one hand, and the convenience of the expert's work, on the other hand, it is proposed to be based on the following provisions:

- The use by experts of methods of qualitative analysis and their interpretation in quantitative measurement.
- Application of the method of individual survey based on the lack of exchange of information between experts. Each expert must have an individual access password to the server to perform expert evaluation and obtain initial information about the evaluation object, but cannot exchange information with other experts. This excludes the dependence of the evaluation results on the dominance of the opinions of the most active and authoritative specialists and ensures the "anonymity" of the experts' opinions.
- Ensuring when agreeing and grouping the final results of a real compromise, taking into account the opinions and level of competence of each expert.
- The application of the fuzzy survey apparatus with the possibility of conducting an expert survey with an orientation to the interpretation of the uncertainty interval in the form of its scale structure.
- To take into account the ability of a person to recognize and form his evaluations within the recommended limits of the Miller number when building the structures of rating scales.(7 ± 2).
- Making the final decision is the prerogative of a person - a team of specialists responsible for the company's policy, who are the initiators of the development and are interested in achieving a high-quality result.

IV. Methodology

Model 1. Morphological analysis of scenario building options based on the base of models. The application of this model provides an opportunity for DM to systematically investing ate possible options for the implementation of risk assessment information technology processes and to make decisions about the feasibility of applying one or another assessment scenario in the existing situational decision-making conditions. The informational basis of the model is M1 (f.3):

$$M1 = (SPR; \{PR_r; M_x\{PR_{irz}\}; \{M_{rx}\ \}\}| i \in I; r = \overline{1, r^*}; z = \overline{1, z^*}; x = 1, x^* \tag{3}$$

Where SPR– a structural model of information technology risk assessment processes, based on which the composition of information technology processes is determined.

〖PR〗 _r- r-th process of information technology.

〖PR〗 _irz- z-th variant of implementation in the i-th information system. r-th process.

M_(r-)- a subset of models of the model base used in the implementation of r-th process.

The implementation of the model takes place in the following stages.

Stage 1. Establishing the composition of information technology processes and determining features when building options for their implementation.

Stage 2. Construction of a morphological "box" of scenario building options based on the base of models (Table I). DM carry out an independent review of all processes and signs of the construction of options and determine promising implementation options for each sign. For each variant of process implementation, a subset of models is established, which is used for its implementation.

Stage 3. Construction of the DM of the implementation scenario based on the synthesis of implementation options for each process. The synthesis takes place on the basis of providing the DM with the opportunity to go through all possible combinations of alternative options for each process in the interface with the system and to stop at the most expedient from the point of view of the situational decision-making conditions.

The peculiarity of the morphological analysis model is its multivariation and the flexibility of building variants based on the "morphological box", which the DM can systematically analyze, replenish and choose on its basis real possible and expedient combinations of implementation of individual processes. It provides an opportunity for the DM to systematically review all possible solutions to this problem, to generate new combinations of building risk assessment scenarios.

The result of the application of model 1 of the DM is the implementation options selected for each process. Within the framework of this article, as a basis, we focus on the analysis of the scenario, which includes the following combination of process implementation options: (1.1; 2.1; 3.1; 4.2; 5.5; 6.5; 7.2). According to the selected scenario, the following models of the model base will be considered [18]:

Model 2. Data flow diagram of scenario implementation.

Model 3. Direct expert assessment of basic indicators of risk analysis.

Model 5. Evaluation of the weighting coefficients of indicators of expected losses.

Model 6. Determination of expected values of loss criteria.

Model 7. Complex assessment of losses based on a set of criteria

Model 9. Risk assessment taking into account the impact on privacy, integrity and availability of data

Model 2. Data flow diagram of scenario implementation. The application of this model is envisaged both in the design and software implementation of information technology for risk assessment, and in the implementation of information technology processes by users. The model is based on the basic principles of DFD modeling. Based on it, data sources and users are determined; the composition of processes and how each process transforms input data into output, the logical sequence of their implementation, which determines the relationship between processes; connections of processes with the basic components of (DSS): database, model base and knowledge base. In fig. 1 presents the implementation data flow diagram for the selected scenario.

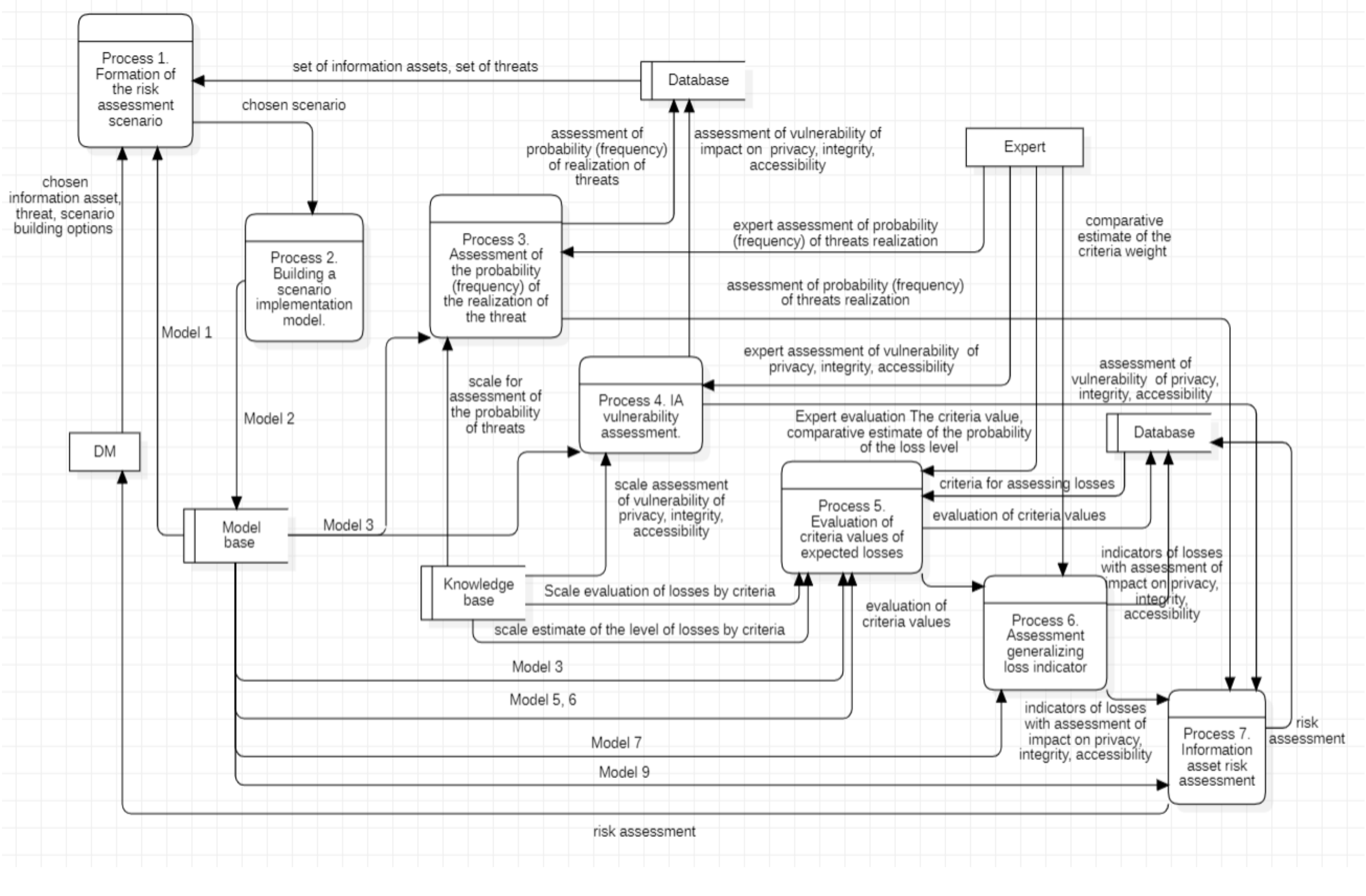
Process 1. Formation of the risk assessment scenario
set of information assets, set of threats
Database
chosen scenario
assessment of probability (frequency) of realization of threats
assessment of vulnerability of impact on privacy, integrity, accessibility
Expert
chosen information asset, threat, scenario building options
Process 2. Building a scenario implementation model.
Process 3. Assessment of the probability (frequency) of the realization of the threat
expert assessment of probability (frequency) of threats realization
comparative estimate of the criteria weight
assessment of probability (frequency) of threats realization
Model 1
expert assessment of vulnerability of privacy, integrity, accessibility
scale for assessment of the probability of threats
Process 4. IA vulnerability assessment.
assessment of vulnerability of privacy, integrity, accessibility
Model 2
Expert evaluation The criteria value, comparative estimate of the probability of the loss level
Database
DM
scale assessment of vulnerability of privacy, integrity, accessibility
criteria for assessing losses
Process 5. Evaluation of criteria values of expected losses
evaluation of criteria values
Model base
Model 3
indicators of losses with assessment of impact on privacy, integrity, accessibility
Knowledge base
Scale evaluation of losses by criteria
evaluation of criteria values
Process 6. Assessment generalizing loss indicator
scale estimate of the level of losses by criteria
Model 3
Model 5, 6
indicators of losses with assessment of impact on privacy, integrity, accessibility
Model 7
Process 7. Information asset risk assessment
risk assessment
Model 9
risk assessment

Fig. 1. Data flow diagrams of the implementation of the risk assessment scenario

TABLE I. MORPHOLOGICAL BOX OF OPTIONS FOR BUILDING SCENARIOS BASED ON THE BASE OF MODELS

Processes of information technology	Variants of implementation of processes using the base of models				
	Option implementation models				
Process 1. Formation of the risk assessment scenario	Formation of the assessment scenario.				
	Model 1. Morphological analysis of scenario building options based on the base of models				
Process 2. Building a scenario implementation model.	Process 2. Building a scenario implementation model				
	Model 2. Data flow diagram of scenario implementation				
Process 3. Assessment of the probability (frequency) of the realization of the threat	Process 3. Assessment of the probability (frequency) of the realization of the threat.				
	Model 3. Direct expert assessment of basic indicators of risk analysis				
Process 4. IA vulnerability assessment.	Option 4.1	Option 4.2	Option 4.3	Option 4.4	
	Process 4.1 Consolidated assessment IA vulnerabilities	Process 4.2. Assessment of IA vulnerabilities by impact on privacy, integrity; accessibility (PIA).	Process 6.3. Vulnerability assessment taking into account composition basic indicators of CVSS vulnerability	Process 6.4. Assessment of vulnerabilities, taking into account the composition basic indicators of CVSS vulnerability, indicators of temporal (time) metrics, CVSS environment metrics	
	Model 3. Direct expert assessment.		Model 3. Direct expert assessment.		
Process 5. Evaluation of criteria values of expected losses	Option 5.1	Option 5.2	Option 5.3	Option 5.4	Option 5.5
	Process 5.1 Consolidated loss assessment based on one criterion	Process 5.2. Consolidated assessment of costs: from violation of privacy, integrity, availability (PIA).	Process 5.3 Evaluation losses according to the Criteria, which correspond to the composition basic indicators of CVSS vulnerability	Process 5.4. Assessment of losses according to criteria that correspond to the composition of basic CVSS vulnerability indicators, temporal metrics, CVSS environmental metrics	Process 5.5. assessment of losses based on a set of established criteria from violations of privacy, integrity, availability, taking into account the probability and departure of different levels of damages
	Model 3. Direct expert assessment.				Model 5 Evaluation of the weighting coefficients of indicators of expected losses. Model 6. Determination of expected values of loss criteria
Process 6. Assessment generalizing loss indicator	Option 6.1	Option 6.2	Option 6.3	Option 6.4	Option 6.5
	Process. 6.1. Evaluation of the generalized indicator of losses on the basis of a large-scale indicator	Process 6.2. Comprehensive assessment of costs from breach of privacy, integrity, availability (PIA).	Process 6.3. Estimation of losses according to the criteria corresponding to the composition basic indicators of CVSS vulnerability	Process 6.4. Risk assessment based on the full set of CVSS vulnerability indicators	Process 6.5 Comprehensive assessment of losses based on a set of criteria.
	Model 6. Estimation of the generalizing indicator of losses based on the aggregated indicator				Model 7. Complex assessment of losses based on a set of criteria
	Option 7.1	Option 7.2		Option 7.3	Option 7.4
Process 7. Information asset risk assessment	Risk assessment based on consolidated indicators	Risk assessment based on aggregated threat assessment and vulnerability and loss assessment indicators, taking into account the impact on privacy, integrity and availability (PIA)		Process 6.3. Estimation of losses according to the criteria corresponding to the composition basic indicator	Process 6.4. Risk assessment based on the full set of CVSS vulnerability indicators

			s of CVSS vulnerability	
	Model 8. Risk assessment based on consolidated indicators	Model 9. Risk assessment taking into account the impact on privacy, integrity and availability of data	Model 10. Risk assessment taking into account basic indicators of vulnerability CVSS	Model 11. Risk assessment based on the full set of CVSS vulnerability indicators

Model 3. Direct expert assessment. The application of this model provides a formalized logical-mathematical apparatus for transforming the expert's qualitative assessments of the values of the basic indicators of risk assessment. The information basis of this model (M3) is proposed to be characterized by the following ratios (f. 4):

$$M3 = (R_{isl}\,;\ V_{islP};V_{islI};V_{islA};\{R_{isl}^{p};V_{islP}^{p};V_{isI}^{p}V_{islA}^{p};\theta_p\}|i \in I, s \in S, l \in L, p = \overline{1,P}, \tag{4}$$

where R_{isl} - probability (frequency)implementation of the lth threat to the s-th asset of the i-th information system;

$V_{islP};V_{islI};V_{islA}$ - vulnerability of the s-th asset of the i-th information system when the l-th threat to privacy is implemented, integrity and availability; – assessment by the p-th expert R_{isl}^{p} probabilities (frequencies)implementation of the lth threat to the sth asset of the ith information system;

$V_{islP}^{p};V_{isl}^{p}V_{islA}^{p}$- evaluation by the p-th expert vulnerability of the s-th asset of the i-th information system when the l-th threat to privacy is implemented, integrity and availability;

θ_p −indicator of competence than expert in the subject area under consideration.

The construction of the model is based on the systematic application of the capabilities of the following methods: direct expert assessment, analysis of the degree of agreement of expert assessments based on the coefficient of variation, the Delphi method, linear convolution of expert assessments.

Implementation of the model involves three stages:

Stage 1. Evaluation of indicators by each expert R_{isl}^{p}(when implementing process 3, option 3), (when implementing process 4, option 4.2).$V_{islP}^{p};V_{islI}^{p}V_{islA}^{p}$

Stage 2. Analysis of the degree of agreement of experts' opinions when evaluating each indicator.

Stage 3. Generalization of expert assessments.

Stage 4. Making decisions on setting the values of indicators R_{isl} (when implementing process 3, option 3), (when implementing process 4, option 4.2).$V_{islP};V_{islI};V_{islA}$

Stage 1. It is implemented on the basis of the method of direct expert assessment, where the expert is tasked with providing an assessment of indicators within the established scale of indicator measurement. The informational basis for the implementation of this stage is the data of the knowledge base that has advisory nature and include the characteristics of the relevant measurement scales. As an example, fragments of the table of scales for assessing the levels of probabilities (frequencies) of the realization of threats (Table II) and the levels of vulnerability of the asset in terms of the impact on privacy, integrity, and availability of data are given (Table III).

When conducting an assessment, the expert must choose the level of the appropriate indicator and set the value of this indicator in the range of the set values of the selected level. So, for example, when assessing a vulnerability in terms of impact on privacy, an expert can choose a very low qualitative level, and to clarify the assessment, choose a quantitative analogue of a qualitative assessment in the range from 0 to 0.2 (0 - excludes the impact on privacy, other assessments in this range establish a measure low impact).

Stage 2. Analysis of the degree of agreement of experts' opinions when evaluating each indicator. When conducting expert evaluations, the task is to optimize the reliability of expert evaluation in the conditions of data uncertainty and the subjective nature of the evaluation. One of the most important optimization conditions is based on the principle of avoiding generalization of evaluation results with a significant spread of evaluations. The goal of the implementation of the second stage of the model is to analyze the degree of dispersion of the evaluation results and to make decisions about the ways of qualitative generalization of experts' evaluations. The degree of dispersion of the expert's evaluations is estimated for each indicator ((R_{isl};, $V_{islP};V_{islI};V_{islA}$);,) based on the coefficient of variation [14, page 106]. If an unacceptable degree of inconsistency of experts' opinions is established when considering one or most of indicators, it is proposed to identify experts who are the authors of marginal estimates [14, Article 111].

Taking into account the arguments of the OPR, the situation is discussed with a group of experts. According to the Delphi method, experts, in agreement with the arguments of the "authors" of the extreme points, are given the opportunity to change their assessments and conduct a second stage of assessment. If an appropriate level of agreement has not been reached after the re-evaluation, the decision on further decision-making steps is made by the ADR.

Stage 3. Generalization of expert assessments. The general results of the assessment of indicators are determined taking into account the opinions of all experts who have passed the consistency check. The values generalized by the group of experts are determined using ratios (f. 5):

$$Q_{isl}\partial = (R_{isl}\,;\ V_{islP};V_{islI};V_{islA})E_i^p = \{e_1^i, e_p^i, \dots, e_{p^*}^i\}Q_{isl}\partial$$

$$Q_{isl}\partial = \sum_{p=1}^{p^*} Q_{isl}\partial p \times \delta_{isl}^{p} \tag{5}$$

Where is the comparative coefficient of expert competence in this expert group (f. 6):

$$\delta_{isl}^{p} = {}^{\theta_p}\!\Big/_{\sum_{p=1}^{p^*}\theta_p} \qquad (6)$$

TABLE II. AN EXAMPLE OF BUILDING A THREAT LEVEL ASSESSMENT SCALE

The name of the threat implementation level	The level of probability (frequency) of threat realization				
	Very low	Low	Average	High	Very tall
Range of values	0-0.25	0.25.-0.5	0.5-0.75	0.75-1	≥ 1
Qualitative characteristics of the probability (frequency) of threat realization	The implementation of this threat is unlikely, no similar cases have been recorded in the last few years	Ability carries out the threat low or source of threat not enough motivated Expected frequency does not exceed one time in 2-5 years	Realization of this threat is potentially possible. An attempt to implement the threat has been recorded once or twice over the past few years	The threat is quite real. Attempts to implement the threat have been recorded several times in recent years	The threat is quite real. Attempts to implement the threat have been recorded several times for the last year

TABLE III. AN EXAMPLE OF BUILDING AN EVALUATION SCALE AND LEVELS OF VULNERABILITY OF THE ASSET IN TERMS OF IMPACT ON PRIVACY

	The level of vulnerability of the asset				
The name of the vulnerability level	Very low	Low	Average	High	Very tall
Range of values	0-0.2	0.2-04	0.4-0.6	0.6-0.8	0.8 – 1.
Qualitative characterization of the threat level in the event of a privacy breach	There is no impact on privacy	There is little disclosure, but the extent of the loss is limited such that no key data is available.	There is significant disclosure, but the extent of the loss is limited such that not all data is available.	There is a disclosure of some restricted information, but the information disclosed has a direct and serious impact	Confidential accuracy of information is not guaranteed

Stage 4. Making decisions on setting the values of indicators R_{isl} (when implementing process 3, option 3), (when implementing process 4, option 4.2). The OPR analyzes the results of the assessment and makes a decision to continue the implementation of risk assessment processes or makes the necessary, from its point of view, changes in the assessment process to improve the reliability of the results obtained.V_{islP}; V_{islI}; V_{islA}.

Model 5 Evaluation of the weighting coefficients of indicators of expected losses. With the application of this model provides a formalized logical-mathematical apparatus for determining the numerical coefficient, a parameter that reflects significance - the relative importance ("weight") of a certain indicator compared to other indicators that affect the assessment of expected losses during risk analysis.

The informational basis of the model is proposed to be characterized by the following ratios $M5$ (f. 7):

$$M5 = \{f_j, \rho_j\}, \{\rho_j^p\}J\}, \{, e_{p:}^{i}\theta_p\}, \left\{W_q, N_q, \beta_{isljP_q}, \beta_{isljI_q}\beta_{isljA_q}\right\},$$
$$\{\beta_{isljP_q}, \beta_{isljI_q}\beta_{isljA_q}\} | i \in I, s \in S, l \in L, p = \overline{1, p^*};\ j = \overline{1, j^*}; q = \overline{1, jq^*} \qquad \textbf{(7)}$$

Wheref_j- criterion of the set set of criteria $F = \{f_1, \dots, f_j, \dots, f_{j^*}\}$;

ρ_j– established on the basis of the application of the model in the implementation of the process (see Fig. 1) "weight" of the criterion, =1;$0 \leq \rho_j \leq 1, \sum_{j=1}^{j^*}\rho_j$

ρ_j^p- "weight" of the criterion, set on the basis of the assessment of the p-th expert during the implementation of the process (see Fig. 1), =1;$0 \leq \rho_j^p \leq 1, \sum_{j=1}^{j^*}\rho_j^p$

$e_{slp:}^{i}$- an expert of the established group of experts $E_i^p = \{e_1^i, e_p^i, \dots, e_{p^*}^i\}$

θ_p – indicator of competence than expert in the subject area under consideration, in the established rating scale;

W_q- the level of assessment of expected costs according to established criteria;

N_q- value of expected losses at the q-th level in the established measurement scale;

$\{\beta_{isljP_q}, \beta_{isljI_q}\beta_{isljA_q}\}$– established on the basis of the application of the model during the implementation of the process (see Fig. 1), the probability of the departure of the expected q-th level of losses according to the j-th criterion as a result of the impact on privacy, integrity and availability of data;

$$0 \leq \beta_{isljP_q} \leq 1, \sum_{q=1}^{q^*}\beta_{isljP_q} = 1;\ 0 \leq\ 1, \sum_{q=1}^{q^*}\beta_{isljI_q} = 1;\ 0 \leq \beta_{isljA_q} \leq 1, \sum_{q=1}^{q^*}\beta_{isljA_q} = 1;$$

$\left\{\beta_{isljP_q}, \beta_{isljI_q}\beta_{isljA_q}\right\}$ – established on the basis of the evaluation of the p-th expert during the implementation of the process (see Fig. 2) the probability of the departure of the expected q-th level of losses according to the j-th criterion as a result of the impact on privacy, privacy, integrity and availability of data:

$$0 \leq \beta_{isljP_q}{}^{p} \leq 1, \sum_{q=1}^{q^*}\beta_{isljP_q}{}^{p} = 1\,; 0 \leq \beta_{isljI_q} \leq 1, \sum_{q=1}^{q^*}\beta_{isljI_q} = 1;\ 0 \leq \beta_{isljA_q}{}^{p} \leq 1, \sum_{q=1}^{q^*}\beta_{isljA_q}{}^{p} = 1.$$

The construction of the model is based on the systematic application of the possibilities of the following methods: analysis of hierarchies (MAH), analysis of the degree of agreement of expert assessments based on the concordance coefficient, the Delphi method, linear convolution of expert assessments. Implementation of the model involves three stages:

Stage 1. The expert's comparative assessment of the significance of the indicators and establishing the "weight" of the indicators in the expert's assessment.

Stage 2. Analysis of the degree of agreement of experts' assessments.

Stage 3. Generalization of expert assessments.

Stage 1. Comparative assessment by an expert of the significance of indicators. In various processes, a comparative assessment of various indicators takes place on the basis of this model. The implementation of the stage is carried out on the basis of the application of the model for evaluating the significance of indicators proposed by the authors, which is outlined in the work [14, pp. 95-104]. As an example of the implementation of the first stage of the model, we will illustrate the construction of matrices of paired comparisons by an expert when assessing the degree of probability of realization of different levels of losses$W_i$when the threat is realized (Table IV). In our example ethe expert considers all levels of damage possible when the threat is realized and provides a comparative assessment of the superiority of one level over others. The informational basis for the implementation of this stage is the data of the knowledge base that has advisory nature and include the characteristics of the corresponding loss measurement scales for each criterion (Table V). We denote classes of levels of damage by , (When assessing expected losses, the expert, using his experience, determines to which of the seven possible levels of damage the realization of a threat to an information asset will lead to according to the criterion.

$$W_i i = \overline{1,7}.z_l^i a_s^i f_j$$

TABLE IV. MATRIX OF PAIRWISE COMPARISONS OF THE PREFERENCE OF THE PROBABILITY OF DEPARTURE OF DIFFERENT LEVELS OF EXPECTED LOSS

Damage level	**Criterion – Consequences relations with clients and partners", impact on data integrity**	W_1	W_1	W_1	W_1	W_1	W_1	W_1	**The probability of departure of loss levels $\beta_{isljI_q}^{p}$**
W_1	Purely optimistic losses	1	1/2	1/2	1/2	1/2	1/2	1/2	0.0738
W_2	Optimistic losses	2	1	1/2	1/2	1/2	1/2	1/2	0.0910
W_3	Low losses	2	2	1	1/2	1/2	1/2	1/2	0.1106
W_4	Average losses	2	2	2	1	1/2	1/2	1/2	0.1332
W_5	High losses	2	2	2	2	1	2	2	0.2375
W_6	Pessimistic losses	2	2	2	2	1/2	1	2	0.1937
W_7	Purely pessimistic losses	2	2	2	2	1/2	1/2	1	0.1603

TABLE V. CHARACTERISTICS OF RELEVANT LEVELS OF LOSSES ACCORDING TO THE CRITERION "CONSEQUENCES RELATIONS WITH CLIENTS AND PARTNERS"

Damage levels		**Range of values**	**Characterization of levels of damage from breach of privacy, integrity and availability of information**
W_1	Purely optimistic losses	0-1	Has no consequences
W_2	Optimistic losses	1-2	Has no tangible consequences
W_3	Low losses	2-4	Leads to a decrease in trust on the part of some customers and partners
W_4	Average losses	4-6	It leads to the loss of trust of some customers or potential customers, a decrease in trust on the part of some partners
W_5	High losses	6-8	Negative information about the company is distributed in Mass media, loss of trust on the part of a significant part of customers and partners
W_6	Pessimistic losses	8-9	Loss of trust on the part of a significant part of customers and partners, wide negative popularity
W_7	Purely pessimistic losses	9-10	Serious deterioration of trust between partners

Stage 2. Analysis of the degree of agreement of experts' assessments. The goal setting of this stage and the principles of implementation are based on the main provisions of the Delphi method. They are defined in the description of stage 2 of model 3. The peculiarity of its implementation in this model is the application of the method of ranking the evaluation results and the assessment of the degree of consistency based on the concordance coefficient. The choice of this approach to the analysis of the degree of agreement of survey results with a more convenient and reliable device for establishing the degree of agreement for the vectors of assessments of each expert [14], [18].

Stage 4. Generalization of expert assessments. The generalized results of the assessment of the weighting coefficients are determined taking into account the opinions of the experts, which were approved by the DM based on the results of the consistency check. The values generalized by the group of experts are determined by analogy with the implementation of stage 3 of model 3 (f. 5-6) $\mathrm{E_i^p} = \{\mathrm{e_1^i}, \mathrm{e_p^i}, \dots, \mathrm{e_{p*}^i}\}\mathrm{Q_{isl}}\,\partial$

Model 6. Determination of expected values of loss criteria. Application of this model provides a formalized logico-mathematical apparatus for establishing expected values of loss criteria. The information basis of the model (M6) it is proposed to be characterized by the following ratios (f. 8):

$$\text{M6}= \{f_j\}, \left\{W_q, N_q, \beta_{isljP_q}, \beta_{isljI_q}\beta_{isljA_q}\right\},\}$$

$$\{\text{Rr}MN_{isljP}, MN_{isljI}, MN_{isljA}\}|\ i \in I, s \in S, l \in L, \text{j=1, 1,.(8)}\overline{j}^{*}q = \overline{q*} \quad (8)$$

Where W_q is the level of assessment of expected costs according to established criteria;

N_q- value of expected losses at the q-th level in the established measurement scale;

$\{\beta_{isljP_q}, \beta_{isljI_q} \beta_{isljA_q}\}$– established on the basis of the application of the model during the implementation of the process (see Fig. 1), the probability of the departure of the expected q-th level of losses according to the j-th criterion as a result of the impact on privacy, integrity and availability of data; $0 \le \beta_{isljP_q} \le 1$,

$$\sum_{q=1}^{q^*} \beta_{isljP_q} = 1;\ \ 0 \le \beta_{isljI_q} \le 1, \sum_{q=1}^{q^*} \beta_{isljI_q} = 1;\ 0 \le \beta_{isljA_q} \le 1, \sum_{q=1}^{q^*} \beta_{isljA_q} = 1$$

Rr-set reliability level of assessment results (0,5<Rr≤1).

As a result of the application of the model in the implementation of process 5 (see Fig. 1), it is proposed to determine the set of indicators of expected costs N_islj, which is considered as a discrete random variable (f. 9):

$$N_{islj} = MN_{isljP};\ MN_{isljI}; MN_{isljA}\}; \{RN_{isljP};\ RN_{isljI}; RN_{isljA}\} \quad (9)$$

where:$\{MN_{isljP};\ MN_{isljI}; MN_{isljA}\}$– mathematical expectation of the assessment of the j-th criterion of losses in case of violation of privacy, integrity and availability of data;

$RN_{isljP};\ RN_{isljI}; RN_{isljA}\}$– estimation of the j-th criterion of losses in case of violation of privacy, integrity and availability of data, which we do not exaggerate with the established level of reliability.

The implementation of the model takes place in two stages:

Stage 1. Establishing a mathematical expectation estimates of the j-th criterion of losses in case of violation of data privacy MN_{isljP} (f. 10), data integrity MN_{isljI} (f. 11) and data availabilityMN_{isljA}:. (f. 12):

$$MN_{isljP} = \sum_{q=1}^{q^*} N_q \times \beta_{isljP_q} \quad (10)$$

$$MN_{isljI} = \sum_{q=1}^{q^*} N_q \times \beta_{isljI_q} \quad (11)$$

$$MN_{isljA} = \sum_{q=1}^{q^*} N_q \times \beta_{isljA_q} \quad (12)$$

Mathematical expectation is the center of distribution of expert's evaluations by levels for each criterion. $W_q f_j$:The meaning of this characteristic is that it defines the most plausible measure of costsand can be considered as a single indicator of expected costs in the conditions significant frequencies of threat repetition $z_l^i \in Z_i$on the information asset $a_s^i \in A_i$.In Table VI, as an example, the data of the distribution of a discrete random variable in the assessment of a group of experts are given.

TABLE VI. DISTRIBUTION OF A DISCRETE RANDOM VARIABLE IN THE ASSESSMENT OF A GROUP OF EXPERTS ON THE LOSS CRITERION "COMMERCIAL INTERESTS OF THE COMPANY" TAKING INTO ACCOUNT THE IMPACT ON THE INTEGRITY OF DATABASE FILES AS A RESULT OF THE THREAT "CHANGE OF SYSTEM PRIVILEGES WITHOUT AUTHORIZATION"

Indexes distribution	Damage level						
	W_1	W_2	W_3	W_4	W_5	W_6	W_7
Range of values	0-1	1-2	2-4	4-6	6-8	8-9	9-10
N_q	0.5	1.5	3	5	7.0	8.5	9
β_{isljI_q}	0.0738	0.0910	0.1106	0.1332	0.2375	0.1937	0.1603

Taking these data into account, we determine This number when analyzing the results of the DM assessment means that the value of expected losses corresponds to the average level of losses $MN_{isljI} = 5{,}9\, W_4$. Mathematical expectation can be considered as a single indicator of cost estimation in conditions significant frequencies of threat repetition threats to the information asset. $z_l^i \in Z_i a_s^i \in A_i$. Then, as is known from the limit theorem of probability theory, the difference between the arithmetic mean of the repetition results and the mathematical expectation approaches zero. In our case, it is impractical for DM to focus only on this criterion. In the event of minor repetitions of the threat, this indicator determines the expected losses, which may not be exaggerated with a probability of 0.5. Therefore, it is considered necessary to present a range of estimates for further analysis of the indicators, which guarantee that the level of damage with the specified OPR reliability is not exceeded$\{RN_{isljP};\ RN_{isljI}; RN_{isljA}\}$Rr.

Thus, in our example, the group of experts foresees all levels of threats, and, in fact, takes into account both optimistic, pessimistic, and pragmatic consequences of the threat's realization for an information asset. In these conditions, in order to improve the results of DM decision-making in conditions of uncertainty, it is proposed to provide these two indicators that take into account other properties of the sample for further analysis. Suppose in our example OPR has set Rr= 0.8. To determine, an analysis of the distribution of damage levels is carried out according to the expert's estimates $RN_{islj\text{Ц}}$ (f. 13):

$$R_{isljI} = \sum_{q=1}^{n} \beta_{isljI_q},\ R_{islj\text{Ц}} \le Rr \quad (13)$$

where n is the ordinal number of the component of the probability vector, which, in the sum with the previous ones, gives a value that satisfies condition (13). For our example = 8.7.

For DM, this means that according to experts' estimates, with a reliability of 0.8, the level of expected losses will not exceed very high losses (W_6) according to the criterion when a threat to an information asset is realized.$W_6 f_j \in F z_l^i \in Z_i a_s^i \in A_i$

Model 7. Complex assessment of losses based on a set of criteria. The application of this model provides a formalized mathematical apparatus for establishing a set of complex indicators of expected losses. The information basis of this work is proposed to be characterized by the following ratios (f. 14):

$$\boldsymbol{M7} = \{\{f_j, \rho_j\}\}_j; \{MN_{isljP};\ MN_{isljI}; MN_{isljA}\}; \{RN_{isljP};\ RN_{isljI}; RN_{isljA}\} |\ i \in I, s \in S, l \in L, j=1,\overline{j^*} \quad (14)$$

As a result of the application of the model in the implementation of process 6 (see Fig. 1), it is proposed to determine the set of indicators of expected losses KN_{isl} (f. 15):

$$KN_{isl}= \{KMN_{islP}; KMN_{islI}; KMN_{islI}; KMN_{isl}\}; \{KRN_{islК};\ KRN_{islI}; KRN_{islA}\ ; KRN_{isl}\} |\ i \in I, s \in S, l \in L \quad (15)$$

whereKMN_{isl} is a generalizing comprehensive indicator of losses in case of breach of privacy, integrity and availability of data where, at the choice of the DM, the mathematical expectation of the assessment of the j-th criterion of losses is taken into account;

KRN_{islP}-a comprehensive indicator of expected losses, where, at the choice of the OPR, the evaluation of the j-th criterion in the event of a violation of data privacy is taken into account, which we do not exaggerate with the established level of reliability;

KRN_{islI} - a complex indicator of expected losses, where, at the choice of the DM, the evaluation of the j-th criterion in case of violation of data integrity is taken into account, which we do not exaggerate with the established level of reliability;

KRN_{islA}- a complex indicator of expected losses, where, at the choice of the OPR, the evaluation of the j-th criterion is taken into account in case of violation of the reliability of the data, which we do not exaggerate with the established level of reliability;

KRN_{isl}- a generalizing complex indicator of losses in case of breach of privacy, integrity and availability of data, where, at the choice of the OPR, the evaluation of the j-th criterion is taken into account, which we do not exaggerate with the established level of reliability.

The implementation of the model takes place in two stages.

Stage 1. Determination of complex indicators by the method of convolution of criteria (f. 16-21):

$$KMN_{islP}=\sum_{j=1}^{j^*} MN_{isljP} \times \rho_j \quad (16)$$

$$KMN_{islI}=\sum_{j=1}^{j^*} MN_{isljI} \times \rho_j \quad (17)$$

$$KMN_{islA}=\sum_{j=1}^{j^*} MN_{isljA} \times \rho_j \quad (18)$$

$$KRN_{islP}=\sum_{j=1}^{j^*} KRN_{islP} \times \rho_j \quad (19)$$

$$KRN_{islI}=\sum_{j=1}^{j^*} KRN_{islI} \times \rho_j \quad (20)$$

$$KRN_{islA}=\sum_{j=1}^{j^*} KRN_{islA} \times \rho_j \quad (21)$$

In Table VII, as an example, we present the data of the evaluation of the indicators of the criteria of expected losses at realization of the threat.

TABLE VII. EVALUATION OF INDICATORS OF EXPECTED LOSSES WHEN THE THREAT IS REALIZED "CHANGING SYSTEM PRIVILEGES WITHOUT AUTHORIZATION" ON THE INFORMATION ASSET "DATABASE FILES"

Indicators of loss assessment	**Loss assessment criteria**				
	Financial	**Consequences relations with clients and partners"**	**Breach of contracts**	**Company image**	**IC malfunction**
ρ_j^p	0.29	0.30	0.20	0.15	0.06
MN_{isljP}	7.2	6.3	6,7	3,4	5
MN_{isljI};	5.4	5.9	4.5	3.2	0
MN_{isljA}	0	0	0	0	0
KRN_{islP};	8.2	6.8	7.4	4.2	6,7
KRN_{islI}	6.5	8.7	5.4	4.4	0
KRN_{islA}	0	0	0	0	0

For our example, the complex indicators of expected losses are equal (Table VIII).

TABLE VIII. COMPREHENSIVE INDICATORS OF EXPECTED LOSSES WHEN THE THREAT IS REALIZED "CHANGING SYSTEM PRIVILEGES WITHOUT AUTHORIZATION" ON THE INFORMATION ASSET "DATABASE FILES"

$\boldsymbol{MN_{islP}}$		$\boldsymbol{MN_{islI}}$	$\boldsymbol{MN_{islA}}$	$\boldsymbol{KRN_{islP}}$	$\boldsymbol{KRN_{islI}}$	$\boldsymbol{KRN_{islA}}$
6,128		4,716	0	6.93	6.235	0

Stage 2. Determination of the generalizing comprehensive indicator of losses.

If the threat has an impact on the violation of several properties, then for further analysis, an indicator characterizing the worst level of loss from the consequences of violations of privacy, integrity and availability of data is determined KMN_{isl} (f. 22) and KRN_{isl} (f. 23):

$$KMN_{isl} = \max(KMN_{islP};\ KMN_{islI}; KMN_{islA}) \quad (22)$$

$$KRN_{isl}= \max(KRN_{islP};\ KRN_{islI}; KRN_{islA}) \quad (23)$$

For our example (see Table 8)

KRN_{isl}= max (6,128; 4,716;0) =6,128; KRN_{isl} = max (6,93; 6,235; 0) = 6,93.

Model 9. Risk assessment taking into account the impact on privacy, integrity and availability of data. The risk is understood as the level of loss that the company will suffer in the event of a threat to a specified information asset using its vulnerability. Model 9 is used in the implementation of the final process of risk assessment technology. The informational basis of this model is proposed to be characterized by the following ratios (f. 24):

$$M8 =\{ R_{isl}\ ; V_{islP}; V_{islI}; V_{islA}\}; \{MN_{isljP};\ MN_{isljI}; MN_{isljA}\}; \{RN_{isljP};\ RN_{isljI}; A\} \{KMN_{islP}; KMN_{islI}; KMN_{islA}; KMN_{isl}\}; \{KRN_{islP}; KRN_{islI}; KRN_{islA}\ ; KRN_{isl}\} |\ i \in I, s \in S, l \in L, j=1,\overline{j^*} \quad (24)$$

As a result of the application of the model during the implementation of process 7 (see Fig. 1), it is proposed to determine the following set of risk indicatorsR_{isl}(f. 25).

$$RR_{isl} = (RM_{isl}; RR_{isl}); (RM_{islP}; RM_{islI}; RM_{islA}); (RR_{islP}; RR_{islI}; RR_{islA}); \{RM_{isljP}; RM_{isljI}; RM_{isljA}\}; \{RR_{isljP}; RR_{isljI}; RR_{isljA}\} | \, i \in I, s \in S, l \in L, j=1,\overline{j^*} \quad (25)$$

Where is a generalized risk indicator that determines the level of damage based on the mathematical expectation of loss assessment indicator (f. 26):RM_{isl}

$$RM_{isl} = \max_{PIA}(RM_{islP}; RM_{islI}; RM_{islA}) \quad (26)$$

RR_{isl}- a generalized risk indicator that determines the level of damage based on risk criteria that will not be exaggerated with the established level of reliability (f. 3127):

$$RR_{isl} = \max_{PIA}(RM_{islP}; RM_{islI}; RM_{islA}) \quad (27)$$

RM_{islP}; $RM_{isl\text{Ц}}$; $RM_{isl\text{Д}}$- risk indicators that determine the level of damage based on the criterion of mathematical expectation of loss assessment in case of violation of privacy (f. 28), integrity (f. 29) and data availability (f. 30):

$$RM_{islP} = R_{isl} \times V_{islP} \times KMN_{islP} \quad (28)$$

$$RM_{islI} = R_{isl} \times V_{islI} \times KMN_{islI} \quad (29)$$

$$RM_{islA} = R_{isl} \times V_{islA} \times KMN_{islA} \quad (30)$$

RR_{islP}; RR_{islI}; RR_{islA}- risk indicators that determine the level of damage on the basis of risk criteria, which will not be exaggerated with the established level of reliability in case of violation of privacy (f. 31), integrity (f. 32) and data availability (f. 33):

$$RR_{islP} = R_{isl} \times V_{islP} \times KRN_{islP} \quad (31)$$

$$RM_{islI} = R_{isl} \times V_{islI} \times KRN_{islI} \quad (32)$$

$$RM_{islA} = R_{isl} \times V_{islA} \times KRN_{islA} \quad (33)$$

RM_{isljP}; RM_{isljI}; RM_{isljA}- risk indicators that determine the level of damage based on the criterion of mathematical expectation of loss assessment according to the specified criterion in case of violation of privacy (f.34), integrity (f.35) and data availability (f.36):

$$RM_{isljP} = R_{isl} \times V_{islP} \times MN_{isljP} \quad (34)$$

$$RM_{isljI} = R_{isl} \times V_{islI} \times MN_{isljI}{}_{isl\text{Ц}} \quad (35)$$

$$RM_{isljA} = R_{isl} \times V_{islA} \times MN_{isljA} \quad (36)$$

RR_{isljP}; RR_{isljI}; RR_{isljA} – risk indicators that determine the level of damage based on the established risk criterion, which will not be exaggerated with the established level of reliability in case of violation of privacy (f.37), integrity (f.38) and data availability (f.39):

$$RR_{isljP} = R_{isl} \times V_{islP} \times RN_{isljP} \quad (37)$$

$$RR_{isljI} = R_{isl} \times V_{islI} \times RN_{isljI}{}_{isl\text{Ц}} \quad (38)$$

$$RR_{isljA} = R_{isl} \times V_{islA} \times RN_{isljA} \quad (39)$$

The informational basis of the analysis of the results of the risk assessment is the data of the knowledge base, which are of a recommendatory nature and include the characteristics of the risk measurement scale (Table IX).

TABLE IX. RISK ASSESSMENT SCALE

Risk level	Range of values	Characteristic
Purely optimistic	0-1	There is no risk. Implementation of the threat is impossible
Optimistic	1-2	There is almost no risk. Successful implementation of the threat is practically impossible, and there are no consequences.
Very low	2-3	The risk can be neglected. Successful implementation of the threat is rare and the consequences are minor.
Low	3-4	The risk is small. The probability of the threat's realization and its consequences are rather small.
Moderate	4-5	Successful implementation of the threat is possible, the consequences will be average
Average	5-6	The risk is serious. The potential realization of the threat exists, the consequences will be sensitive.
High	6-7	The risk of threat realization is high. The realization of the threat is rather possible, the consequences are significant.
Pessimistic	7-8	The risk of threat implementation is very high, successful threat implementation is possible, and the consequences will most likely be catastrophic
Purely pessimistic	8-10	The risk and probability of realization of the threat are very high. The consequences with a global impact are extremely high, which can cause a complete collapse of the system, the restoration of stable operation is almost impossible

So, as an example, we will consider the following data to determine the totality of risk indicators taking into account the impact on the integrity of database files as a result of the threat "Changing system privileges without authorization"

Probability of threat realization R_{isl}= 0.357, the vulnerability of the asset in terms of impact on privacy V_{islP} =0,607, for integrity $V_{islI} = 0{,}235$; and availability $V_{islA} = 0$; expected losses when the threat is realized are given in the table. 8.

As a result of the implementation of the model, the following set of indicators characterizing the risks of breaching the privacy, integrity and availability of data were established.

RM_{islP}=1.33; RM_{islI}= 0,396; $RM_{islA} = 0$; RR_{islP}=1,5;
RR_{islI}=0,523; $RR_{islA} = 0.$; RM_{isl} =1,33; $RR_{isl} = 1{,}5$.

The values of the indicators show that in the conditions of averaging the expected costs in the implementation of the threat based on estimates of mathematical expectation, the maximum risk indicator, reflecting the consequences of the implementation of the threat, associated with a violation of the privacy of information, indicates an optimistic level of risk. Even the application of cost estimates that guarantee the established level of reliability corresponds to an optimistic level of risk.

V. Results

The obtained results of the study indicate that the approaches, models and methods that make up a single information technology of risk assessment create an effective toolkit of influence on the quality solution of one of the most important and urgent problems of information security risk minimization. The versatility of the built models allows you to easily apply the obtained tools in practice. Taking into account the problem of conceptual uncertainty and weak structuredness of the data characterizing them, it is proposed to use system-related models based on:

- three-level approach to risk management: "organization - business processes - information systems";
- variant approach of building alternative assessment scenarios based on the method of morphological analysis (Table 1);
- the system formalized connection of such components of the DSS as "decision-making process" - "data base" - "knowledge base" - "model base" (Fig. 1).
- the dominant role of the "human factor" in the evaluation and decision-making process;
- the principles of the maximum possible formalization of processes;
- validity of application and expansion of possibilities of logical-mathematical methods of expert assessment, interactive mode of working with tools convenient for a specialist.

When the group of experts evaluates the probability and (frequency) of the realization of threats to a specified information asset, its vulnerability in terms of impact on privacy, integrity; availability of data, a model of direct expert assessment is proposed based on the appropriate correction of the DM levels of the assessment scales (4)-(6). When assessing the expected losses from the realization of the threat, various factors of the consequences of its possible departure are taken into account on the basis of an established set of criteria and scales for their evaluation (7)-(14), while the proposed assessment of different levels of potential losses and the probabilities of their departure (15)-(21), which significantly increases the reliability of the estimate of expected losses from the implementation of the threat in conditions of incomplete data certainty.

A range of indicators is provided in the final assessment of the risk of DM. Some determine the level of damage based on the criterion of weighted average loss assessment, the other are risk indicators that focus the attention of ODA on the guaranteed results of not exaggerating losses with an established level of reliability (24)-(39).

Taking into account the variety of problems and the weak structure of the data that characterize them, the considered scenario of formalizing risk assessment is built on the basis of systemically connected models based on the use of dominant expert opinion, the validity of application and the expansion of the possibilities of mathematical and logical methods of expert assessment for the formalization of adoption processes solutions In these conditions, in order to increase the effectiveness of the obtained results, special attention was paid to the selection of a group of experts, namely, analysis, evaluation and formalized consideration of the degree of their competence (5)–(6).

VI. Discussions

The advancement of information security has seen significant expansion, driven mainly by the escalating intricacy of cyber threats and the importance of digital assets. The article "A Comprehensive Examination of Information Security Risk Assessment Models" offers an in-depth analysis of diverse models for assessing risks in information security, specifically designed to address the complex requirements of this field. The objective of this discourse is to elaborate on the perspectives presented in the article while also establishing connections and differentiating it from other relevant scholarly contributions in the discipline.

The article emphasizes the significance of implementing a robust risk assessment framework to safeguard the confidentiality, integrity, and availability of information systems. The National Institute of Standards and Technology (NIST) has been a leading institution in the development of a comprehensive approach to risk management. The NIST Special Publication 800-37 outlines a comprehensive framework for addressing security and privacy concerns throughout the system life cycle. It highlights the significance of continual monitoring and improvement in effectively managing risks [1]. This statement agrees with the perspective presented in the paper, which emphasizes the necessity of employing dynamic models capable of adjusting to the continuously changing landscape of threats.

The writing further explores the complexities associated with different risk assessment approaches. The CRAMM user guide is a risk analysis and management tool created by the United Kingdom Central Computer and Telecommunication Agency (CCTA) [3]. The approach described is based on the cybersecurity guidelines established by the United Kingdom government. It offers a comprehensive structure for the discovery, assessment, and mitigation of risks. The OCTAVE technique is a significant framework for assessing information hazards [4]. The study underscores the flexibility and comprehensiveness of risk assessment models, aligning with the fundamental concepts of both CRAMM and OCTAVE.

The article highlights the need for risk assessment models tailored to individual regions and industries. The MEHARI 2007 and Magerit v2 2006 exemplify customized models designed to cater to the distinct requirements of information systems in France and Spain, respectively [5,6]. The models presented in the article support the idea that although generic models provide essential knowledge, customized models provide more detailed insights tailored to the specific demands of a particular location or industry.

The evaluation of vulnerabilities is an essential aspect of risk assessment. The Common Vulnerability Scoring System (CVSS) offers a standardized methodology for assessing the severity of system vulnerabilities [7]. By incorporating a standardized approach into the risk assessment procedure, companies can enhance their ability to prioritize vulnerabilities according to their potential effect.

Nevertheless, it would have been advantageous for the essay to go into the financial ramifications associated with information security threats. For example, the research conducted by Dai et al. on detecting online credit card theft sheds light on the increasing financial vulnerabilities linked to cybersecurity. It emphasizes employing hybrid frameworks to address these challenges [8]. Moreover, the scholarly contributions of K. Bury and Andrii Kaminskyi offer comprehensive analyses of the financial hazards associated with banking organizations and propose conceptual frameworks for quantifying these risks [9,12]. These resources highlight the significance of technological vulnerabilities and the potentially catastrophic financial consequences of security breaches.

The significance of personnel in the context of information security risk management should be considered. According to the research conducted by Yurii Khlaponin et al., the risks related to reliance on essential staff significantly impact information security [13]. This viewpoint emphasizes the complex nature of hazards related to information security, which includes both technological and human factors.

The article offers a comprehensive examination of several models utilized in evaluating information security risks, providing valuable insights. The utilization of several techniques and frameworks highlights the need to adopt a comprehensive and flexible strategy in the management of information security threats. Incorporating financial and human factors into the risk assessment process can enhance an organization's ability to defend against cyber threats, in addition to the essential role played by the technical parts of these models. As the digital landscape undergoes continuous transformation, it becomes imperative to adapt the concepts and approaches employed for its protection.

VII. CONCLUSIONS

The approach to the implementation of human-machine information technology for assessing information security risks based on a systemically linked base of expert assessment models with the use of modern capabilities of decision-making support systems was studied. The considered models are built with the aim of providing assistance to the ODA in decision-making based on the gradual implementation of risk assessment processes based on a formalized toolkit. Each assessment session provides for the formation of OPR based on the morphological analysis of options for the information technology work scenario, which, from the user's point of view, more closely correspond to the situational conditions that have developed in the company when making decisions.

The obtained results of experimental calculations indicate that conducting a risk assessment, which ends with the determination of a set of indicators, based on the proposed formalized apparatus, does not cause any inconvenience. It enables the DM to base its evaluations on the analysis 〖RR〗

_is probability of threat implementation, vulnerability information system from its implementation to the impact on privacy, data integrity and availability; expected losses when the threat is realized.

Special attention is paid to the issue of formalization of the rules of surveying experts, the effectiveness of models, methods of obtaining and processing their estimates, generalization of different opinions as a crucial component of information technology and the guarantee of a significant increase in the reliability of the results.

It should be noted that the work pays attention to the assessment of risks within the framework of the selected information asset of the company in the event of the realization of a certain threat, and the toolkit for the systematic linking of the assessment of the impact of various types of threats in terms of grouping assets according to the degree of impact has not yet been proposed. This question is planned to be refined in the following studies.

REFERENCES

[1] NIST: ‘Risk Management Framework for Information Systems and Organizations A System Life Cycle Approach for Security and Privacy’, Special Publication 800-37. Revision 2, 2018

[2] Potii, O., Gorbenko, Y., Zamula, O., and Isirova, K.: ‘Analysis of methods for assessing and managing cyber risks and information security’, Radiotekhnika, 2021, 3, (206), pp. 5-24

[3] CRAMM: ‘Risk Analysis and Management Method, United Kingdom Central Computer and Telecommunication Agency’, CCTA user guide, 2001

[4] OCTAVE: ‘methodology for evaluating information risks’, Electronic resource, 2020

[5] MEHARI: ‘Concepts and Mechanisms’, Club de la Sécurité de l'Information Français., 2007

[6] PÚBLICAS, M.D.A.: ‘MAGERIT – version 2. Methodology for Information Systems Risk Analysis and Management’, Book-I: The Method, 2006

[7] FIRST.Org, I.: ‘Common Vulnerability Scoring System version 3.1: Specification DocumentCVSS Version 3.1’, CVSS Release, 2019

[8] Dai, Y., Yan, J., Tang, X., Zhao, H., and Guo, M.: ‘Online Credit Card Fraud Detection: A Hybrid Framework with Big Data Technologies’, in Editor (Ed.)^(Eds.): ‘Book Online Credit Card Fraud Detection: A Hybrid Framework with Big Data Technologies’ (2016, edn.), pp. 1644-1651

[9] Bury, K.: ‘ Classification of financial risks of banking institutions’, Naukovyy visnyk Natsionalnoho universytetu bioresursiv i pryrodokorystuvannia Ukrainy,, 2010, 154, (3), pp. 49–56

[10] Nosratabadi, S., Pintér, G., Mosavi, A., and Semperger, S.: ‘Sustainable Banking; Evaluation of the European Business Models’, SSRN Electronic Journal, 2020

[11] Berg, H.P.: ‘Risk management: procedures, methods and experiences’, RT&A, 2010, 1, (17), pp. 79–95

[12] Kaminskyi, A.: ‘Conceptual approaches to measuring financial risks’, Finansy Ukrainy, 2006, 5, pp. 78-85

[13] Yurii Khlaponin, O.I., Nameer Hashim Qasim, Hanna Krasovska, Kateryna Krasovska: ‘Management risks of dependence on key employees: identification of personnel.’, Workshop on "Cybersecurity Providing in Information and Telecommunication Systems" (CPITS 2021), 2021, pp. 295-308

[14] O. Izmailova, H.K., K. Krasovska & V. Zaslavskyi: ‘ Assessing the Variety of Expected Losses upon the Materialization of Threats to Banking Information Systems.’, Information & Security: An International Journal, 2020, 45, pp. 89-118

[15] Cristian, A.: ‘Practical methods for information security risk management’, Informatica economica, 15, (1), pp. 151-159

[16] Lavrenyuk S.I., S.A.Y., Lavrenyuk A.M.: 'Multi-criteria risk analysis violation of information security in GRID systems', Programming problems., 2010, (Special issue 2-3), pp. 507-512

[17] Izmailova O.V., K.G.V., Krasovska K.K.: 'Module for estimating expected losses in the information security risk management system of a construction company.', Ways to increase the efficiency of construction in the conditions of the formation of market relations. , 2022, 50, (1), pp. 81-92

[18] Olha Izmailova, S.P., Iryna Melnyk, Kateryna Krasovska: 'Improving the reliability of the values of the significance of criteria in determining the market value of real estate objects,' Upravlinnia rozvytkom skladnykh system, 2017, 29 pp. 109-118