Information & Security

Published since 1998

O. Izmailova, H. Krasovska, K. Krasovska &
V. Zaslavskyi, vol. 45 (2020): 89-118
https://doi.org/10.11610/isij.4506

ISSN 0861-5160 (print), ISSN 1314-2119 (online)

Research Article

Assessing the Variety of Expected Losses upon the Materialisation of Threats to Banking Information Systems

Olha Izmailova [1] (✉), ***Hanna Krasovska*** [2], ***Kateryna Krasovska*** [2], ***Volodymyr Zaslavskyi*** [2]

[1] *Kyiv National University of Construction and Architecture, Kyiv, Ukraine*
http://www.knuba.edu.ua/eng/

[2] *Taras Shevchenko National University of Kyiv, Kyiv, Ukraine*
http://www.univ.kiev.ua

ABSTRACT:

The article addresses the problem of estimating the expected losses of a bank when information security threats to functioning computer systems materialize. A scenario approach to solving the problem is developed based on multi-criteria decision-making methods, taking into account quantitative and qualitative indicators and expert assessment, and applying the analytic hierarchy process for comprehensive assessment of expected losses in probabilistic terms. That allows to take into account different levels of the hierarchy of criteria and the weight of their impact on the calculated results. The process of estimating the probability of materialization of various threats under accepted standards and situational conditions, the actions of the attacker and the consequences on the bank's functioning is formalized. Expert assessments are grouped with control over the sufficiency of the degree of logic and dispersion of opinions of each expert, compliance with the established requirements for the degree of consistency of opinions of the group of experts, assessment and formalized consideration of the degree of their competence. The process of assessing expected losses is presented as a daily business process of the functioning of the bank's security system.

ARTICLE INFO:

RECEIVED: 17 OCT 2020
REVISED: 22 DEC 2020
ONLINE: 30 DEC 2020

KEYWORDS:

information system security, expected loss levels, multi-criteria approach, expert assessment

✉ Corresponding Author E-mail: olga.v.izmailova@gmail.com

Introduction

Ensuring effective information security of information and analytical systems is a fundamental basis for the successful functioning of banks, banking and payment systems, which are indicated as a critical infrastructure of the country.[1,2] The implementation of business processes is impossible without the use of a variety of secure information, analytical and computer systems. Ways and tasks of ensuring information security of such systems based on different conditions, target tasks of ensuring the level of protection, require the implementation of different types of alternative solutions for the organization of security.[3,4] To justify the required level of protection, many factors that form the basis for performing functional tasks of the organization and standards on information security problems are taken into account.[5,6] In the course of their activities, banks analyse and assess risks regarding the degree of their impact and threats that arise, and constantly set tasks for improving and optimizing the structure of security and cybersecurity systems. Optimization of security systems involves generating a variety of compromise solutions, among which some allow certain risks to be accepted, and this can be used by banks to increase their profits.

The applied task of risk analysis of information-analytical and computer systems is to identify hazards-sources of risks, determine probability of occurrence and materialization of threats, assess the consequences and losses from the materialization of the threat. In this regard, the accuracy and reliability of the qualitative and quantitative assessment of the bank's expected losses from the consequences of materialized threats directly affect ensuring the level of information security of the bank.

Analysis of Referenced Sources

There is an urgent need to improve risk management systems in banks and payment systems as caused by a variety of new factors of influence and types of fraud, which are actively and dynamically developing due to global digitalization, uncertainty and complexity of the external and internal environment of their functioning.

Modern innovative ideas and practical recommendations of many domestic and foreign scientists and researchers on risk management are common in scientific publications. In works [7-10], the results of research on the search for solutions for effective risk management and countering threats are presented, which are the basis for specific business processes of banks and payment systems and their implementation in relevant information and analytical systems.[11,12] A system of risk classification of banks and payment systems is proposed, their analysis and implementation features in the financial sphere and information systems of financial institutions were carried out.[13-15] Mathematical models and algorithms for risk analysis in banking activities and problems of ensuring the security of banks and payment systems have also been explored.[16-19]

In modern conditions, risk management is increasingly moving away from the strict target setting for avoiding and minimizing risks and aims at forming compromise solutions – the possibility of taking a certain level of risk and using it in favour of the bank. This is due to the fact that when implementing business processes, various types of risks arise, some of which require reduction, others – analysis and accounting. The risk management system organically covers all business processes and implements effective risk management as a component of the overall information security system of financial systems.

From a systemic point of view, risk assessment is based on taking into account three of its components:

$$R = p_1 \cdot p_2 \cdot w, \qquad (1)$$

where p_1 is the probability of a threat; p_2 is the vulnerability of the object to the threat; w is loss assessment during threat materialization.

When implementing information and analytical systems for banks, a scenario approach is used, which is based on the use of alternative models and methods to support business processes and provide security systems.[16, 20, 21] The basics of this approach were designed in the development of decision support systems (DSS),[22,23] where it was important to combine models and methods, rules for forming information and logical connections between the components of the DSS, which made it possible to implement alternative scenarios and the sequence of solving problems.

Mathematical models and methods of risk assessment are defined in the NIST SP 800-30 Risk Assessment Manual,[24] and the OWASP Risk Assessment Methodology.[25] They provide for assessing the level of losses and the probability of risk realization on a qualitative scale without its quantitative interpretation. More complex methods, such as OCTAVE, Allegro, MEHARY, NS Magerit,[26] take into account the influence of information resource relationships, and are used when forming security measures, databases of possible threats. A special feature of these works is that the loss is assessed based on a single generalizing indicator. It is assessed without formalized structuring of expert opinions on individual criteria that are components of the aggregated loss indicator.

The argument for a significant positive impact on improving the results of assessment based on structuring the expert opinions in assessing loss based on many criteria have already been a subject of research studies.[27,28]

When implementing the scenario approach, an important component of the effectiveness of risk management is the perfection of models and methods for determining the cost of losses that may arise when materializing certain threats and risks for the bank's information and analytical systems. The accuracy of the assessment of possible loss is a certain measure of risk assessment reliability, the reliability of identifying the most vulnerable points of hazards and minimizing risk to use measures to achieve established standards and guarantees.

In scientific publications, the assessment of the cost of loss is considered as a complex multi-criteria indicator, characterized not only by financial losses. A theoretical model for assessing factors that determine compromise was proposed based on two criteria – the level of banking competition and the level of risk at the credit level.[29] The amount of loss was considered as the sum of binomially distributed random variables that depend on the parameters of attacks and defences, combining economic losses, time and recovery costs.[30]

The analysis of current research areas shows that the assessment of possible loss departs from the standard of accounting only for financial costs, requires the use of large amounts of statistical data collected from various sources: similar cases, information from various organizations (government agencies, computer emergency response teams, industry associations, banks, publications and electronic information resources). On their basis, quantitative indicators of losses can be formed, methods of qualitative assessment of information risks can be improved, taking into account the human factor, mathematical models and methods of expert assessment. However, the reliability of these data is not guaranteed, which requires further research. The question of estimating the value of information actually lost as a result of incidents remains open. From the point of view of a systematic approach, it is necessary to define the principles of development and requirements for alternative scenarios, models and methods that are the basis for their implementation in threat research and assessment of expected losses.

Problem Statement

Based on the analysis of references, it is possible to conclude that today the possibilities of accepting a particular level of loss in the materialization of threats arising in the course of banking activities are not sufficiently studied. To do this, it is necessary to develop appropriate tools for conducting an expert assessment of losses from materialization of threats during banking processes to further classify the estimates obtained. The results of the assessment of losses from materialization of a particular threat can be used for further decision-making on the possibility of making a projected level of loss when materializing a threat to improve the efficiency of banking activities. Applying this approach will allow us to find a rational compromise between the need to strengthen security measures in banking activities to reduce losses and effective business conduct, since quite often the introduction of strict restrictions can negatively affect the bank's competitive ability in the market.

The problem statement can be formalized as follows. Let the bank operate a fixed set of information systems (IS) $i \in I = \{1, 2, ..., k^*\}$. Each IS has a set of information assets: $A_i = \left\{a_1^i, a_2^i, \dots, a_s^i, \dots, a_{s_i'}^i\right\}, i \in I$.

An information asset is an information or resource (information, technical, software) that is subject to protection in the bank, its information networks and systems.

Examples of the bank's $a_s^i \in A_i, i \in I$ assets are:

- actual information assets: databases and database files, system documentation, user manuals, training materials, technical maps for the support and maintenance of the bank's IS, archival data, data about the bank's customers and their transactions, etc.;
- software assets: system and application software, development tools and utilities;
- physical assets: computer equipment, communication equipment, other technical equipment, furniture, premises, etc.;
- services: information, computing, communication services, etc.

Then: $A = \bigcup_{i \in I} A_i$, a set of information assets of all IS in the bank. For each IS $i \in I$, a finite set of possible threats is known for a certain time:

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

It is important to note that multiple threats can be sorted into specific threat classes, for example, as follows: $Z_i z_l^i \in Z_i$

- for implementation of: encroachment on confidentiality; interference with data integrity; system failure (malfunction).
- according to the method of influencing the system: obtaining unauthorized access to system objects; connecting to the system by creating secret channels.
- by the nature of the impact on the system: active impact is when the system state changes as a result of the threat materialization; passive impact is when the system state remains unchanged as a result of the threat implementation, but the attacker gets access to the confidential sensitive information.
- as a result of security errors: when implementing security tools, the possibility of materializing a threat was not taken into account; incorrectly organized management and control over personnel actions; errors in software algorithms.
- by attack tools: standard software; specially designed programs, etc.

The main examples of threats $z_l^i \in Z_i$ to the bank's information security are:

- fraud with financial instruments by bank employees;
- collusion of clients with bank employees or collusion between bank employees;
- abuse of authority by bank employees;
- theft, loss, destruction and disclosure of confidential information;
- forgery of documents;
- providing false information about individuals and purposes of financial interaction;

- fraud with financial instruments;
- cyber fraud;
- unauthorized access to computer systems and networks;
- introduction of fraudulent programs into computer systems, etc.

Denote by $Z = \bigcup_{i \in I} Z_i$, a set of all possible threats to all bank's IS. The threat sets for different IS may differ, but the same threat may be for many IS. The bank's IS and their information assets do not function in isolation, because they are united by a set of business processes performed in the bank, so a certain set of threats at a certain point in time is determined, because the impact and interference in the bank's activities are constant and change with the advent of new information technologies.

Denote by $G = \bigcup_{i \in I} G_i$ the set of functional tasks of the bank, the performance of which is assigned to the IS that ensure the implementation of the bank's business processes, where $G_i = \{g_1, g_2, \dots, g_i, \dots, g_{i^*}\}$, a set of business processes in the bank's IS that ensure the achievement of functional tasks. Thus, $g_i = \left\{g_1^i, g_2^i, \dots, g_m^i, \dots, g_{m_i'}^i\right\}, i \in I$ contains a set of all subtasks necessary for the functioning of business processes.

To assess losses in materialization of threats to the bank's IS information assets, it is necessary to define a set of assessment criteria.

Let $F = \left\{f_1, \ \dots, f_j, \dots, f_{j^*}\right\} = \left\{f_j, j \in J\right\}, J = \{1, 2, \dots, j^*\}$, a set of criteria used to assess losses when materializing threats in information systems. The values of the criteria f_j are given on the sets A_i and Z_i.

In this case, the values of the criterion $f_{ij}^{ls} = f_j\left(z_l^i, a_s^i\right)$, $z_l^i \in Z_i$, $a_s^i \in A_i$, functions f_{ij}^{ls} can be set tabular. We denote by ρ_j , $j \in J$ are the given weighting factors ρ_j of each criterion, so that $\rho_j \geq 0, \sum_{j \in J} \rho_j = 1$.

Examples of criteria f_j are: "financial loss," "damage to reputation," "possibility of functioning of the information system," etc. The set of evaluation criteria f_j may vary depending on the information system, information asset and threat under consideration.

To calculate the overall level of risk R using formula (1), it is necessary to assess the expected losses w that arise when materializing threats to the bank's IS information assets. Expected losses are considered as a complex indicator that is determined based on certain loss functions:

$$w = \sum_{j \in J} \rho_j \cdot f_{ij}^{ls}, \tag{2}$$

where ρ_j is the weight (measure of influence) of each criterion of the lowest level of the hierarchy, taken into account when evaluating the final results of losses for all IS assets; f_{ij}^{ls} is a generalized criterion indicator for the criterion $f_j \in F$ when materializing a threat $z_l^i \in Z_i$ on an information asset $a_s^i \in A_i$.

It is proposed to calculate the values of criterion indicators $f_{ij}^{ls} = f_j(z_l^i, a_s^i\ )$ using human-machine tools, that is, a group of experts with a summary of the estimates obtained therefrom.

Let: $E_i^p = \{e_1^i, e_p^i, \dots, e_{p^*}^i\}$, $p \in P = \{1,2, \dots, p^*\}$ be multiple experts participating in the assessment. In practice, a set of possible experts is determined who take part in assessing the expected losses when materializing a threat from the set Z_i for an information asset A_i according to the criterion f_j: $E = \bigcup_{p\in P} E_i^p$.

The formation of a group of experts takes into account their awareness of the IS under consideration, so the set of experts may differ depending on the bank's IS. It is also important to note that for each expert, an indicator of their competence can be set $\theta_{e_p^i}$, which can be taken into account when forming a focus group of experts, as well as when calculating the final estimates of expected losses.

The scenario for estimating expected losses is based on the systematic application of the capabilities of the following methods: expert assessment (Saaty's analytic hierarchy process (AHP),[31] Delphi method[22]), linear convolution of criteria and evaluation of the characteristics of random variables. The approach to solving this problem consists of the following steps, the details of which are discussed in the next section "General scheme of problem solving":

Step 1. Assessment by focus group experts E_i^p of the probability of serving possible levels of loss for each criterion $f_j \in F$ when materializing a threat $z_l^i \in Z_i$ to an information asset $a_s^i \in A_i$.

Step 2. Estimation of expected values of loss criteria indicators f_{ij}^{ls}.

Step 3. Generalized assessment of the group of experts of the expected criterion indicators of loss $f_{ij}^{ls} = f_j(z_l^i, a_s^i\ )$.

Since the expert works in conditions of incomplete certainty of data during the assessment, its opinion is based not only on existing knowledge about decision-making in these conditions, but also requires a professional intuitive analysis of the multi-factor future consequences of the threat materialization. At the same time, it is necessary to take into account different situational conditions of the system's functioning and possible discrepancies in the attacker's target intentions. Therefore, the scenario provides for the creation of a formalized tool for determining by the expert various options for the consequences of the threat materialization, assessing the probability of their departure and taking into account the impact on the generalized assessment of expected losses. In this case, it is proposed to introduce seven classes of possible losses. The number of classes may vary depending on the conditions of the task at hand. Their number may be higher or lower. There is a concept of the psychological limit of a person's ability to simultaneously distinguish a certain number of objects by some property. This limit is equal to the Miller interval 7$\pm$2, that is, 9 points are enough to create a scale on which these objects can be compared. Therefore, to simplify the perception of experts and conduct a qualitative assessment, it is proposed to use seven classes.

We denote the classes of loss levels by W_i, $i = \overline{1,7}$ (Fig.1). When assessing the expected losses, the expert, based on his or her experience, determines which of the possible seven levels of loss will lead to the materialization of a threat z_l^i to an information asset a_s^i under the criterion f_j. So, for example, the owner of an information resource can easily indicate the cost of the terminated contract or the cost of equipment and media, but one is not actually able to name the exact cost of the lost information. Thus, using qualitative indicators: small, mediocre, large, etc., the expert will be able to formally and unambiguously express one's opinion.

The expert is given the opportunity to assess the following seven levels of loss:

W_1 – purely optimistic losses (non-volatile and extremely low losses that will not change the overall state of the system);

W_2 – optimistic losses (low impact – low losses that can change the overall state of the system, but will not affect its functioning);

W_3 – low losses (losses with the minor impact that can change the overall state of the system and even slightly impair its functioning);

W_4 – average losses (losses with a weighted average impact that can change the overall state of the system and its functioning, but it takes little time to restore operation);

W_5 – high losses (losses with a significant impact, change the overall state of the system and significantly affect its functioning, the recovery time of the normal state of the system is quite long);

W_6 – pessimistic losses (losses with a significant impact, can radically change the overall state of the system, have a huge impact on its functioning, the time and possibility of recovery is difficult to estimate, but recovery is possible);

W_7 – purely pessimistic estimates (losses with global impact are extremely high, which can lead to a complete collapse of the system, and it is almost impossible to restore stable operation).

Since the proposed gradation represents a certain qualitative scale, a scale for structuring preferences for each level is also established W_i, that is, their limit and average values in the range from 0 to 1 (Fig.1): $\{W_i^{min}, W_i^{mid}, W_i^{max}\}$, where $W_i^{mid} = {W_i^{min} + W_i^{max}}\big/_2$ (Fig.1). For example, this distribution is defined in the range from 0 to 1, which is divided into 7 ranges according to the number of loss levels that may occur before the scenario starts. This range is

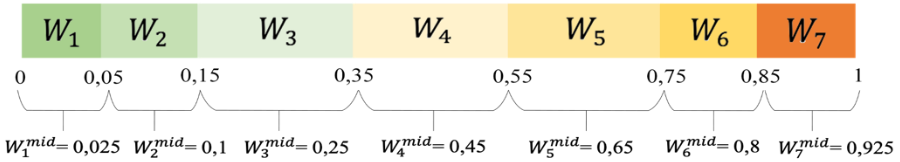

Figure 1: Scale for classifying the level of estimates of expected losses.

determined by the decision-maker (DM) – the responsible employee of the bank. In this case, it is proposed to use a larger step of 0.2 for median classes and a smaller step for boundary classes, since their influence is much more significant. The scale is determined to obtain the expected value W_i, based on the value w, formula (2). So, for example, if as a result of calculations based on expert estimates $w = 0.4$, then the estimate of expected losses is based on a scale (Fig.1), will be at the level W_4.

The implementation of the scenario is based on a systematic analysis of the following components:

- multiple protection objects – IS information assets A;
- multiple threats Z with a certain loss value W_i when materialization threats;
- sets G – functional tasks of the bank, the performance of which is assigned to the IS, ensuring the implementation of the bank's business processes;
- use of qualitative analysis methods with their interpretation in quantitative measurement in a systemically related human-machine procedure in conditions of incomplete data certainty;
- the losses in the materialization of threats are assessed taking into account different criteria F for expected costs.

The following principles of scenario construction are proposed:

- rationality and validity, timeliness and efficiency;
- rationality of asset decomposition levels, threats, criteria and their completeness and reliability;
- rationality of the compromise between the level of decomposition, completeness of the information and the cost of resources for implementation;
- rational use of intuition, knowledge and experience of a human expert; DM – a responsible employee of the bank who makes the final decision;
- rational selection and systematic linking of methods for implementing task stages;
- the expected losses are assessed for the established IS information asset of a certain level of hierarchy from the materialization of a threat of certain type;

- the basis of assessment is human-machine technology, which is based on the use of expert assessment methods;
- the dominant role of expert assessments is determined and the rule is established – making a final decision is the prerogative of a person – a team of specialists responsible for the bank's security policy. At the same time, decision-making should be based on professionalism, awareness, intuition, experience of the DM and experts, so reasonable requirements for the composition of the group should be determined;
- loss factors identified as the most significant in various operating conditions of the system are taken into account. For example, loss related to violation of legal requirements; financial loss from loss of information value; damage to the bank's reputation, etc.;
- for each criterion, weight is set ρ_j – a measure of the significance of the impact of threats on the value of an asset for each criterion;
- criteria indicators are formed by experts based on both qualitative and quantitative data, most of which have latent properties.

When conducting expert assessments, the task is to optimize the reliability of expert assessment in conditions of data uncertainty and the need to anticipate the consequences of threat materialization. To this end, a survey of various experts provides for:

- application of the individual survey method due to the lack of information exchange between experts;
- ensuring the inadmissibility of direct rejection of the individual assessment of each expert;
- avoiding generalization of evaluation results with a significant spread of ratings;
- providing an opportunity for the expert to identify a full range of opinions from purely pessimistic to optimistic;
- ensuring that when coordinating and grouping final results, it is possible to find a real compromise, taking into account the opinions and level of competence of each expert.

Having defined the basic components of script construction, it is possible to build a basic hierarchy (Fig. 2), which is a graphical representation of the problem under consideration. The number of such hierarchies depends on the number of IS $i \in I = \{1,2,\dots,k^*\}$ under consideration.

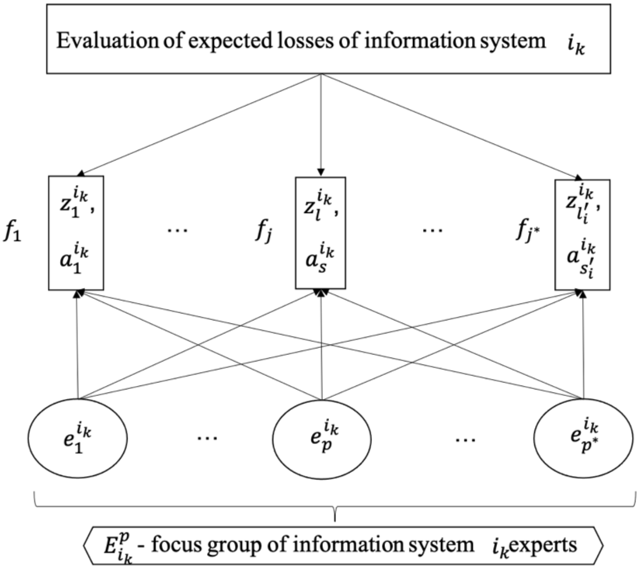

Figure 2: Hierarchy of the task of assessing IS expected losses i_k.

General Scheme of Problem Solving

Step 1. Assessment by focus group experts E_i^p of the probability of serving possible levels of loss for each criterion $f_j \in F$ when materializing a threat $z_l^i \in Z_i$ to an information asset $a_s^i \in A_i$.

For an expert assessment, the AHP method is used,[40] which has proven to be an effective mathematical tool for a systematic approach in the study of weakly structured decision-making problems. The advantage of the AHP method is its ability to "visualize what can happen" in the obligatory condition of gradually clarifying and consolidating (focusing) the conclusions of various experts on something single. According to this method, priority solutions are selected using pairwise comparisons of undefined components. To represent the results of estimates in quantitative terms, a scale of pairwise comparisons is presented in (Table 1).[31]

The expediency of using a discrete scale "1-9" to assess a comparative measure of the probability of different levels of loss from materialization of a threat is determined on the basis of the following prerequisites:

1. The expert is given the opportunity to estimate the results and the probability of serving different levels of consequences, the qualitative differences of which are significant in practice, and their consideration, from one's point of view, increases the reliability of the assessment results.

Table 1. Scale of pairwise comparisons.

Degree of predominance of the probability of one level of loss over another	**Degree of predominance importance (significance)**
Equal probability. No predominance	1
Weak predominance in probability. Weak predominance.	3
Significant or strong probability predominance. Strong predominance.	5
Very strong or significant probability predominance. A very strong predominance.	7
Absolute probability predominance.	9
Interim evaluation of the degree of predominance	2, 4, 6, 8

2. The properties of a human expert are taken into account, which allow us to comfortably conduct qualitative distinctions of measures of the probability of waiting for the levels of loss to objects by certain degrees at a professional level.

3. The AHP pairwise comparison scale is used (Table 1).

In general, the expert is proposed to construct a matrix of pairwise comparisons of the degree of probability of appearance of different levels of losses W_i according to the criterion $f_j \in F$ when materializing a threat $z_l^i \in Z_i$ to an information asset $a_s^i \in A_i$. For the problem under consideration, 7 possible loss levels are established, so it is possible to construct a matrix of pairwise comparisons of the following form (Table 2), where α_{mq} is the preference rating given by the expert:

Table 2. Matrix of pairwise comparisons.

Level of loss/ Level of loss	W_1	…	W_q	…	W_7
W_1	α_{11}	…	α_{1q}	…	α_{17}
…	…	…	…	…	…
W_m	α_{m1}	…	α_{mq}	…	α_{m7}
…	…	…	…	…	…
W_7	α_{71}	…	α_{7q}	…	α_{77}

Pairwise comparisons are made in terms of determining the degree of superiority of one level of loss $W_m$over another by an expert W_q. At the same time, the expert's qualitative intuitive estimates are converted into quantitative ones, which are expressed in integers. If the level W_m dominates W_q, then the matrix element corresponding to the line W_m and column W_q is filled with an integer according to Table 1, in this case, the element corresponding to the line W_q and column W_m is filled with the inverse number, i.e., a fraction $\alpha_{qm} = {}^1/_{\alpha_{mq}}$. If the level W_m does not dominate W_q, then the opposite happens. If it is considered equal W_q and W_m equally likely, then put one in both positions. This matrix must have the property of inverse symmetry.

A special feature of using the AHP method in the scenario under consideration is the foresight and provision of tools to exclude those levels of loss that cannot occur from the expert's point of view. The probability of their departure is defined as zero, and they are excluded from comparative evaluation models. This allows the expert to reflect the opinion of even the only possible level of loss when materializing a threat.

We denote as $\beta^p = ({\beta^p}_{W_1}, {\beta^p}_{W_2}, \dots, {\beta^p}_{W_i}, \dots, {\beta^p}_{W_7})$ – the vector of alternative weights W_i in the expert's estimates. In this case, condition (3) must be met, as follows: the vector component ${\beta^p}_{W_i}$ is the probability of obtaining the loss level calculated and based on the estimates of the preference ratio filled in the cells of the matrix of pairwise comparisons by the expert $e_p^i \in E_i^p$:

$$0 \le {\beta^p}_{W_i} \le 1, \sum_{i=1}^{7} {\beta^p}_{W_i} = 1. \tag{3}$$

For example, let's assume that an expert compares the degree of superiority of the level of expected losses on the information asset "file database" when materializing a threat of copying information by the criterion – financial loss from the loss of information value (Table 3). The expert considers all levels of loss possible when materializing a threat and conducts a comparative assessment of the advantage of one level over others.

After performing all pairwise comparisons for elements of neighbouring levels, we calculate the probability of serving each loss level ${\beta^p}_{W_i}$ (2) as follows:

1) We define the normalized vector of local priorities:

$$a_m = \sqrt[7]{\prod_{q=1}^{7} a_{mq}}.$$

2) We normalize the components of a vector a_m by dividing each component by the sum of all the components of this vector:

Table 3. Matrix of pairwise comparisons of predominance of the probability of different levels of expected loss over others.

Level of loss	**Criterion - the financial loss in case of loss of information value**	W_1	W_2	W_3	W_4	W_5	W_6	W_7	β^p
W_1	Purely optimistic losses	1	2	5	5	5	4	3	0,3452
W_2	Optimistic losses	1/2	1	3	3	3	3	3	0,2184
W_3	Low losses	1/5	1/3	1	1/4	1/4	1/4	1/4	0,0338
W_4	Average losses	1/5	1/3	4	1	1/4	1/3	1/3	0,0546
W_5	High losses	1/5	1/3	4	4	1	1/3	1/3	0,0811
W_6	Pessimistic losses	1/4	1/3	4	3	3	1	1/3	0,1100
W_7	Purely pessimistic losses	1/3	1/3	4	3	3	3	1	0,1569
Total		2,68	4,67	25	19,3	15,5	11,9	8,25	1

$$\beta^p{}_{W_i} = \frac{a_m}{\sum_{m=1}^{7} a_m}.$$

According to the theoretical provisions of the AHP, there may be a situation of the inconsistency of the judgments of an expert or a group of experts in pairwise comparisons. The occurrence of inconsistency is not only allowed as an integral part of the method, but it also raises the question of diagnosing the causes and consequences of the inconsistency of expert assessments, improving and clarifying them. However, a violation of these coherences indicates a possible illogical assessment. The first step is to calculate the matrix of normalization of expert ratings. So, in Table 5 for our example, a normalization matrix is given that illustrates the shift in expert estimates in assessing the advantage of loss levels. The normalized value H_{mq} is defined by:

$$H_{mq} = \frac{a_{mq}}{\sum_{m=1}^{7} a_{mq}}. \quad (4)$$

The data of the normalized matrix indicate that $a_{mq} \neq {\beta^p}_{W_m} / {\beta^p}_{W_q}$ this indicates that the expert's assessments are not completely consistent. Therefore, the task is to diagnose the cause of inconsistency and make a decision on applying or rejecting the results of the expert's assessment. To check the consistency of the expert's opinions, the following metrics are used:[32]

- CI – consistency index;
- RI – stochastic consistency coefficient, which depends on the dimension of the matrix and takes into account its inverse symmetric construction (Table 4);
- CR – consistency assessment.

Table 4. Stochastic consistency coefficient.

Matrix size	2	3	4	5	6	7	8	9	10
RI	0	0,58	0,9	1,12	1,24	1,32	1,41	1,45	1,49

Also, to calculate the consistency estimate CR, you need to find the eigenvalue λ_{max} of the matrix (Table 5) using the formula (5) and the eigenvector $\lambda_{\max m}$ of the matrix (6). At the same time, in conditions of the inconsistent agreement of opinions λ_{max}, the value deviates from the order of the matrix, which in this case is equal to 7.

$$\lambda_{max} = \sum_{m=1}^{7} \lambda_{\max m} \times {\beta^p}_{W_m}, \quad (5)$$

Where $\lambda_{\max m}$ is the maximum eigenvalue of the matrix (Table 5) at each loss level:

$$\lambda_{\max m} = \sum_{q=1}^{7} a_{mq} \cdot {\beta^p}_{W_q} / {\beta^p}_{W_m}. \quad (6)$$

The next step is to determine the value CI and CR:

$$CI = {(\lambda_{max} - \mathrm{n})} / {n - 1}, \quad (7)$$

$$CR = CI/RI, \quad (8)$$

Table 5. Normalization matrix.

Level of loss	Criterion - the financial loss in case of loss of information value	W_1	W_2	W_3	W_4	W_5	W_6	W_7	Total	β^p	$\lambda_{\max m}$
W_1	Purely optimistic losses	0,37	0,43	0,2	0,26	0,32	0,34	0,36	2,28	0,3452	7,36
W_2	Optimistic losses	0,19	0,21	0,12	0,16	0,19	0,25	0,36	1,49	0,2184	7,79
W_3	Low losses	0,07	0,07	0,04	0,01	0,02	0,02	0,03	0,27	0,0338	8,17
W_4	Average losses	0,07	0,07	0,16	0,05	0,02	0,03	0,04	0,44	0,0546	8,08
W_5	High losses	0,07	0,07	0,16	0,21	0,06	0,03	0,04	0,65	0,0811	8,21
W_6	Pessimistic losses	0,09	0,07	0,16	0,16	0,19	0,08	0,04	0,80	0,1100	7,85
W_7	Purely pessimistic losses	0,12	0,07	0,16	0,16	0,19	0,25	0,12	1,08	0,1569	7,76
Total		1	1	1	1	1	1	1	7	**CI**	0,117
										RI	1,32
										CR	0,089
										λ_{max}	7,704

A sign of an unacceptable level of inconsistency in the expert's assessments is the condition $CR > 0{,}1$.

The value $CR = 0{,}089$ obtained based on formulas (7), (8) confirms, in our example, a sufficient level of consistency in the expert's assessment and the possibility of using the evaluation results at the next stage of scenario implementation.

Step 2. Estimation of expected values of loss criteria indicators f_{ij}^{ls}.

Based on the results of the first step of the scenario, the probability $\beta^p = ({\beta^p}_{W_1}, {\beta^p}_{W_2}, \dots, {\beta^p}_{W_i}, .., {\beta^p}_{W_7})$ of receiving each level of costs is determined. Each level of loss is characterized by the corresponding interval of a pre-set scale (Fig. 1). The generalized value of expected losses according to the expert's estimates $e_p^i \in E_i^p$ for the criterion $f_j \in F$ on an information asset $a_s^i \in A_i$ when materializing a threat $z_l^i \in Z_i$ will be considered as a discrete random variable $V_{e_p^i}^j$. The most likely level of expected losses W_i, based on the expert's estimates, is proposed to be determined based on a set of basic characteristics of random variables: the mathematical expectation of estimating losses $MN_{e_p^i}^j$ for each criterion $f_j \in F$, variance $DN_{e_p^i}^j$, coefficient of variation of estimates $U_{e_p^i}^j$ and the result that will be achieved with a sufficient level of confidence in the opinion of the DM NN.

To calculate the mathematical expectation $MN_{e_p^i}^j$, previously defined values are used W_i^{mid}, as well as the corresponding probabilities $\beta^p = ({\beta^p}_{W_1}, {\beta^p}_{W_2}, \dots, {\beta^p}_{W_i}, .., {\beta^p}_{W_7})$ calculated from expert estimates (Table 6).

We determine the mathematical expectation $MN_{e_p^i}^j$ of estimating losses when materializing a threat $z_l^i \in Z_i$ for an information asset $a_s^i \in A_i$ for each criterion $f_j \in F$:

$$MN_{e_p^i}^j \; = \sum_{i=1}^{7} W_i^{mid} {\beta^p}_{W_i}. \tag{9}$$

Table 6. Distribution line of a discrete random variable W_i^{mid} in the expert's $e_p^i \in E_i^p$ evaluation.

Distribution indicators/ Level of loss	W_1	W_2	W_3	W_4	W_5	W_6	W_7
W_i^{mid}	0,025	0,1	0,25	0,45	0,65	0,8	0,925
β^p	0,3452	0,2184	0,0338	0,0546	0,0811	0,1100	0,1569

Mathematical expectation (9) is the centre of distribution of expert ratings by level W_i for each criterion f_j. For our example, its value is $MN^j_{e^i_p} = 0.3493$. This number for the DM means that the value of expected losses, that is $V^j_{e^i_p}$, corresponding to the expert's estimates $e^i_p \in E^p_i$ for the criterion $f_j \in F$ on an information asset $a^i_s \in A_i$ when materializing a threat $z^i_l \in Z_i$, will be at the level with insignificant impact W_3.

The mathematical expectation is not only the centre of distribution of expert estimates, but, in fact, can be considered as a final estimate. However, this value can be the only indicator for the previous stage of evaluation only if the expert's ratings are slightly scattered. In conditions where the expert estimates wide intervals of loss levels in anticipation of the future consequences of a threat, it is considered appropriate for the decision-maker (DM) to present a value $V^j_{e^i_p}$ with the addition of an indicator $VN^j_{e^i_p}$ that guarantees that the level of loss will not exceed with a certain DM's confidence NN.

$$V^j_{e^i_p} = \left\{MN^j_{e^i_p};\ VN^j_{e^i_p}\right\}. \tag{10}$$

So, in our example, the expert assumes all levels of threat, and, in fact, takes into account both optimistic, pessimistic, and pragmatic consequences of materializing a threat for an information asset. Under these conditions, to improve the results of decision-making by the DM in conditions of uncertainty, it is proposed to provide these two indicators for further analysis, taking into account other properties of the sample, including scattering indicators.

The degree of dispersion of expert estimates is evaluated based on the coefficient of variation U_{e_l} determined based on the ratio:

$$U^j_{e^i_p} = \frac{\sqrt{DN^j_{e^i_p}}}{MN^j_{e^i_p}}, \tag{11}$$

where $DN^j_{e^i_p}$ is the variance of the expert's estimates calculated as follows:

$$DN^j_{e^i_p} = \sum_{i=1}^{7}(W_i^{mid} - MN^j_{e^i_p})^2 \beta^p{}_{W_i}. \tag{12}$$

The degree of scattering will be considered weak if $U^j_{e^i_p} < 10\%$; if $U^j_{e^i_p}$ from 11-25%, then average; and significant when $U^j_{e^i_p} > 25\%$. In our example, the variance is $DN_{e_p^i}^j$ =0.1324, the coefficient of variation is $U_{e_p^i}^j$ =1.0418, which indicates a large dispersion of the expert's estimates. Experience shows that a large value of the coefficient of variation is an essential feature for the DM of the expediency of decomposing the criterion under consideration into component criteria and conducting additional iterations of evaluation based on them. Thus, in our example, the expert assesses the level of expected financial losses. Total financial losses are considered as a criterion for a lower level of decomposition. A high level of scattering of estimates is recommended to be considered as a sign of the feasibility of further decomposition of the criterion. For example, it is advisable to make an assessment based on the following criteria: financial losses in the implementation of the bank's business processes, financial losses from the loss of copyright in development, financial losses in the calculation of wages. Another way is to make a decision by the DM on whether it is appropriate to take into account in decision-making an indicator $VN_{e_p^i}^j$ that will be achieved with a sufficient level of confidence, NN from the DM's point of view.

Let's say the DM set NN to = 0.8. To determine this $VN_{e_p^i}^j$, an analysis of the distribution of loss levels is carried out according to the expert's estimates.

It is necessary to find such $VN_{e_p^i}^j$ that:

$$VN_{e_p^i}^j = \sum_{i=1}^{n} \beta^p{}_{W_i}, \qquad (13)$$

$$VN_{e_p^i}^j \leq NN, \qquad (14)$$

where NN is the established DM's confidence level, which in our example is 0.8, and n is the sequence number of the component of the probability $\beta^p{}_{W_i}$vector β^p, which in sum with the previous ones according to (13) gives a value that satisfies condition (14). For our example $VN_{e_p^i}^j$ = 0.73. Thus, the result of the expert's assessment of the value $V_{e_p^i}^j$ according to (10) is: $V_{e_p^i}^j = \{0{,}3493; 0{,}73\}$.

For the DM, this means that according to the expert's estimates $e_p^i \in E_i^p$, with a probability of 0.8, the level of expected losses will not exceed high losses (W_5) according to the criterion $f_j \in F$ when materializing a threat $z_l^i \in Z_i$ to an information asset $a_s^i \in A_i$. Since several experts are involved in the assessment, the next step is to calculate the generalized estimate and get the value $f_{ij}^{ls} = f_j(z_l^i, a_s^i)$.

Step 3. Summary assessment of the expected loss criteria by the expert group $f_{ij}^{ls} = f_j(z_l^i, a_s^i\,)$.

The task is to summarize the estimates based on the criterion $f_j \in F$ for materialising a threat $z_l^i \in Z_i$ to an information asset $a_s^i \in A_i$, which were obtained for each expert from the group of experts $E_i^p \in E$. In other words, the result of solving this problem will be the result $f_{ij}^{ls} = f_j(z_l^i, a_s^i\,)$ for the criterion f_j, generalised by the group of experts E_i^p. At the same time, a ranking procedure is proposed that allows the DM to find a rational compromise in the assessments of experts, taking into account the full range of their opinions and excluding unjustified rejection of individual assessments. To implement this procedure, the main idea of the Delphi method [22] is used. According to the ideas of the Delphi method, the procedure for grouping results proposed in this scenario is based on the following provisions:

- conducting a survey of experts by individual assessment, provided that there is no exchange of information between experts;
- following the principles and approaches of the group random sampling, a prerequisite for the possibility of generalizing results is the assessment and analysis of the sufficiency of consistency measure of experts' opinions;
- conducting consistency analysis and determine boundary estimates, if necessary;
- analysis by each expert of the results of the group assessment obtained and argumentation of their opinions by the "authors" of extreme assessments;
- enabling experts to repeat the survey procedure;
- making a decision by the DM to move to the definition of integrated assessment while achieving a sufficient degree of coherence of expert opinions. In conditions of insufficient consistency, the DM makes one of the alternative solutions: the transition to a comprehensive assessment without taking into account the opinions of the authors of “extreme” assessments, if their number does not exceed the established limit (for example, 20 %), or the postponement of the assessment process;
- establishing a comprehensive assessment, taking into account the level of competence of each expert.

In this scenario, it is considered rational to analyse the degree of consistency of expert opinions based on the basic results of expert evaluation. An approach is proposed to check the degree of consistency of expert assessments results based on their ranking.[33] Let's illustrate the content of the approach by using the example of processing the results of assessments by five experts $E_i^p = \{e_1^i, e_2^i, e_3^i, e_4^i, e_5^i\}$. Let's assume that when assessing the level of loss according to the criterion f_j for materializing a threat z_l^i to an information asset a_s^i, the following results were obtained $\beta^p{}_{W_i}$ (Table 7).

Based on the data from Table 7, a matrix of ranking evaluation results is formed as presented in Table 8.

We denote the rating of the assessment as: $R_{W_i}^p$, where p is the ordinal number of the expert $e_p^i \in E_i^p$ whose estimates are considered, and W_i is the level of loss $i = \overline{1,7}$.

Ranking is carried out as follows: rank 1 is assigned to the level of loss W_i that is achieved with the highest degree of probability $\beta^p{}_{W_i}$ (according to the expert's estimates), rank 2 – to the next highest value, etc. If the expert evaluates the degree of probability of different levels in the same way, then the same arithmetic mean values are given.

Table 7. Results of evaluation of the probability of occurrence the levels of loss by experts.

Expert e_l/ Probability of occurrence of the levels of loss	W_1	W_2	W_3	W_4	W_5	W_6	W_7
$\beta^1{}_{W_i}$	0,3452	0,2184	0,0338	0,0546	0,0811	0,1100	0,1569
$\beta^2{}_{W_i}$	0,3580	0,346	0,041	0,012	0,1112	0,1314	0,022
$\beta^3{}_{W_i}$	0,244	0,2512	0,1133	0,054	0,0812	0,1133	0,1431
$\beta^4{}_{W_i}$	0,3506	0,2115	0,0390	0,0653	0,0967	0,1636	0,1214
$\beta^5{}_{W_i}$	0,2251	0,1834	0,051	0,1121	0,1231	0,2113	0,094

We also denote the total rank for the loss level W_i as R_{W_i}:

$$R_{W_i} = \sum_{p=1}^{5} \beta^p{}_{W_i}. \quad (15)$$

Table 8. Evaluation results ranking.

Expert/ Probability of occurrence of the levels of loss	W_1	W_2	W_3	W_4	W_5	W_6	W_7
$\beta^1{}_{W_i}$	1	2	7	6	5	4	3
$\beta^2{}_{W_i}$	1	2	5	7	4	3	6
$\beta^3{}_{W_i}$	2	1	4,5	7	6	4.5	3
$\beta^4{}_{W_i}$	1	2	7	6	5	3	4
$\beta^5{}_{W_i}$	1	3	7	5	4	2	6
Total rank (R_{W_i})	6	10	30,5	31	24	16,5	22

The coefficient of concordance (consistency) of expert opinions K is calculated,[33] which reflects the ratio of the maximum possible variance of expert ratings (with full consistency of expert opinions when ranking results) and the real variance:

$$K = \frac{12S}{P^2(n^3-n)-n\sum_{p=1}^{5}T^{l}}, \tag{16}$$

where: $S = \sum_{i=1}^{7}(R_{W_i}^{p} - R^{mid})^2$, $R^{mid} = 0{,}5P(n+1)$, $T^p = \sum_{i=1}^{m}(t^3 - t)$, P are the number of experts, n is the number of loss levels S_i, t is the number of repetitions of rank $R_{W_i}^{p}$ in the expert ranking e_p^i, m is how many times in the expert ranking e_p^i there was a repetition of rank $R_{W_i}^{p}$.

The value of the concordance coefficient *K* is in the range from 0 to 1, a higher value determines a higher level of consistency of expert opinions. If the experts' opinions are fully consistent, the concordance coefficient *K* will be equal to one, and if the experts' opinions are completely inconsistent, it will be zero. The limit value $K^{\text{гр}}$ that is considered sufficient is set by the DM. As a rule, a value $K^{\text{гр}} \geq 0{,}6$ is recommended. If $K > K^{\text{гр}}$, the experts' opinions are considered consistent. For our example $K = 0{,}803$, which determines a sufficient level of consistency of experts' opinions.

If the concordance coefficient *K* is less than 0.6, this indicates the need for the DM to take additional actions to improve the evaluation results, namely, to analyse the causes of inconsistency and search for ways to eliminate them.

If an unacceptable measure of the inconsistency of experts' opinions is established when considering one or more criteria, it is proposed to identify experts who are the authors of marginal estimates. The average value $X_{W_i}^{mid}$ of experts' ratings for each W_i is calculated without taking into account the limit values, that is, the ratings of those experts who made unacceptable inconsistencies:

$$X_{W_i}^{mid} = \frac{R_{W_i} - ({\beta^{min}}_{W_i} N^{min} + {\beta^{max}}_{W_i} N^{max})}{P - (N^{min} + N^{max})},$$

where N^{min} is the number of experts who provided minimum marginal estimates ${\beta^{min}}_{W_i}$, N^{max} is the number of experts who provided maximum marginal estimates ${\beta^{max}}_{W_i}$. Deviations ∇_{min} and $\nabla_{max}$are defined: $\nabla_{min} = X_{W_i}^{mid} - {\beta^{min}}_{W_i}$, $\nabla_{max} = {\beta^{max}}_{W_i} - X_{W_i}^{mid}$. Experts who have given marginal estimates in which the values ∇_{min} or ∇_{max} exceed the permissible deviation value predetermined by the DM ∇ are invited to argue their point of view. Taking into account these arguments, the DM discusses the situation with a group of experts. According to the Delphi method, experts, when agreeing with the arguments of the authors of extreme points, are given the opportunity to change their estimates and conduct a second evaluation stage. If the appropriate level of consistency of views has not been achieved after re-evaluation, the decision on further decision-making is made by the DM.

The final results of loss assessment according to the established criteria are formed taking into account the opinions of all experts who have passed the consistency check. Generalized by the group of experts $E_i^p = \{e_1^i, e_p^i, \dots, e_{p^*}^i\}$, the values of the mathematical expectation $MN_{E_i^p}^j$ of the expected result of the loss, the variance of estimates $DN_{E_i^p}^j$ and the value of the result $VN_{E_i^p}^j$ that will be achieved with a set level of confidence are determined using the relations:

$$MN_{E_i^p}^j = \sum_{p=1}^{P} MN_{e_p^i}^j \alpha_{e_p^i}, \tag{17}$$

where $\alpha_{e_p^i}$ is the comparative coefficient of expert competence in this expert group, and P is the number of experts:

$$\alpha_{e_p^i} = \frac{\theta_{e_p^i}}{\sum_{p=1}^{P} \theta_{e_p^i}}, \tag{18}$$

where $\theta_{e_p^i}$ is the expert's competence indicator in the assessment scale from 0 to 100.

Table 9. Results of evaluations of an expert group.

Exp-ert code	$\boldsymbol{\theta_{e_p^i}}$	$\boldsymbol{\alpha_{e_p^i}}$	**Probability of occurrence of the level of loss ($\boldsymbol{W_1 - W_7}$)**							$\boldsymbol{MN^j_{e_i^i}}$	$\boldsymbol{VN^j_{e_p^i}}$
$\boldsymbol{e_1^i}$	100	0,244	0,35	0,218	0,034	0,055	0,081	0,110	0,157	0,35	0,73
$\boldsymbol{e_2^i}$	80	0,195	0,36	0,346	0,04	0,012	0,111	0,131	0,022	0,43	0,55
$\boldsymbol{e_3^i}$	80	0,195	0,24	0,251	0,113	0,054	0,081	0, 113	0,143	0,41	0,7
$\boldsymbol{e_4^i}$	75	0,183	0,35	0,212	0,04	0,065	0,097	0,163	0,121	0,47	0,65
$\boldsymbol{e_5^i}$	75	0,183	0,23	0,183	0,05	0,112	0,123	0,211	0,094	0,48	0,85
			Generalized indicators							**0,45**	**0,7**

$$DN^{j}_{E_i^p} = \sum_{p=1}^{P} DN^{j}_{e_p^i} \alpha_{e_p^i}, \tag{19}$$

$$VN^{j}_{E_i^p} = \sum_{p=1}^{P} VN^{j}_{e_p^i} \alpha_{e_p^i}. \tag{20}$$

Table 9 shows the results of evaluating the generalized indicator of financial costs on the information asset "file database" when materializing the threat of copying information, which is determined taking into account the assessments of five experts with the established level of competence.

When determining the complex indicator of expected loss (2), the mathematical expectation $MN^{j}_{E_i^p}$ of the expected result of the loss and the value of the result $VN^{j}_{E_i^p}$ that will be achieved with the level of confidence set by the DM will be a generalized indicator $V^{j}_{E_i^p} = \{MN^{j}_{E_i^p}; VN^{j}_{E_i^p}\}$ (where $f_{ij}^{ls} = MN^{j}_{E_i^p}$) of the expected loss for each criterion. So, for example, according to the obtained values, the generalized criterion indicator f_{ij}^{ls} will have a value of 0.42. This means that the expert group believes that the expected loss will be at the same level W_4, i.e., average losses (Fig. 1), but since $VN^{j}_{E_i^p}$ = 0.69, with a certain degree of confidence $NN = 0{,}8$, the losses will not exceed W_5, that is high losses.

Conclusions

The information technology developed from a system perspective for implementing scenarios for solving the actual problem of assessing expected losses in the organization of information security of banks can be used in the study of security problems for various organizational systems.

Taking into account the variety of problems and the weak structure of the data that characterize them, the scenario is built based on systemically related models and methods based on the use of dominant expert opinion, the validity of the application and the expansion of the possibilities of mathematical and logical methods of expert assessment to formalize decision-making processes.

In order to increase the effectiveness of the results obtained, special attention should be paid to:

1) selection of a group of experts, namely, analysis, evaluation and formalized consideration of the measure of their competence (17)-(20), (Table 9);
2) monitoring the sufficiency of the measure of the logic of experts' opinions (3)-(15), (Table 4, 5), the degree of dispersion of assessments of an individual expert (11), (12) and compliance with the established requirements for the degree of opinions consistency from different experts (16);
3) when assessing the possibility of losses, take into account not only the expected financial losses, but also the generalized indicator of expected losses, based on the entire set of criteria. In particular, taking into account the multi-factor consequences of the materialization of each threat on the asset under consideration.

The proposed method of grouping the results of loss assessment by various experts, based on the main principles of the Delphi method, provides additional opportunities for the DM when searching for a rational compromise in expert assessments, taking into account the full range of their opinions (Table 7, Fig. 2). At the same time, formalized control of the degree of consistency of their estimates is provided based on mathematical analysis of the results by ranking grades (15), (16), (Table 8). In conditions of violation of the degree of consistency, based on the analysis of the results, "authors of extreme points" are identified, which are subjects of an unacceptable level of branching of estimates $X_{W_i}^{mid}$, ∇_{min} and ∇_{max} and a 'mechanism' for smoothing the evaluation results is applied.

It should be noted that this scenario has not yet presented a method for assessing the weight of criteria and methods for auditing the competence of experts in the dynamics of their work based on the accumulation of relevant statistical material. These methods are planned to be developed in further studies of the proposed scenario.

The article presents the basic provisions for constructing a scenario for solving the problem of estimating expected losses that arise when materializing threats to the bank's IS. The developed approach is implemented in the form of information technology that systematically connects mathematical models and methods of expert assessment (AHP, Delphi), multi-factor assessment using the linear convolution of criteria, and a comprehensive assessment of the expected characteristics of losses as probabilistic quantities. The task of estimating the probability of serving possible levels of loss for each criterion by an expert is based on the use of the hierarchy analysis method. The determining factor in improving the effectiveness of evaluation is the peculiarity of the proposed process implementation technology and mathematical and logical apparatus, which allow the expert to take into account sets of criteria of different levels of hierarchy, determined qualitatively and numerically.

The developed approach, models and methods used by the expert in assessing the expected values of the loss criterion indicators are aimed at increasing the reliability of the results obtained. This is achieved because it is possible to choose evaluation options based on different approaches to processing expert estimates. The choice of finishing option is the prerogative of the DM. A special feature of the proposed method is that to make a decision, the DM gets the opportunity to be guided by the results of analysing the degree of dispersion of expert assessments and influence the reliability of the results to find a rational compromise. The criterion for the validity of generalization of results for the DM is a measure of the consistency of expert opinions, determined based on the concordance coefficient. Expert compromise assessments are formed by the DM taking into account the full range of expert opinions and excluding unjustified rejection of individual assessments.

If the value of the concordance coefficient is low, estimates are iteratively matched with the discussion of negative results and deviations, according to the decision of the DM, of unjustified “limit” estimates. A significant lever for improving the generalized assessment reliability is to take into account the professional competence of each expert, which is determined by a point scale.

References

[1] Volodymyr Zaslavskyi, “Monitoring and Risks Analysis in Payment Systems,” *Social Risks* 2 (2004): 224-270. – in Russian.

[2] D.S. Biryukov and S.I. Kondratov, *Green Paper on Critical Infrastructure Protection in Ukraine: Collected Materials from International Expert Meetings* (Kyiv: National Institute for Strategic Studies*,* 2015). – in Ukrainian.

[3] A.V. Anisimov, V.A. Zaslavskyi and O.M. Fal, *Fundamentals of Information Security and Information Protection in the Context of Euro-Atlantic Integration of Ukraine: Scientific-methodological Manual* (SE "Scientific and Production Center “Euroatlanticinform,” 2006). – in Ukrainian.

[4] Volodymyr Zaslavsky, "Type–Variety Principle and Decision of Complex Systems with a High Price of Failure," *Bulletin of the University of Kiev, Series: Physics and Mathematics* 1 (2006): 136-147. – in Ukrainian.

[5] Hanna Krasovska, Olha Izmailova, and Kateryna Krasovska, "Approach to Build a Break-out Scenario for Solving Task on Supporting Decision-making Assessment of Real Estate," *Upravlinnia rozvytkom skladnykh system* 16 (2013): 86–95. – in Ukrainian.

[6] Yurii Khlaponin and Olha Izmailova, "Approach to Ensure Protection of Corporate Information Systems in Construction," *Upravlinnia rozvytkom skladnykh system* 31 (2017): 126–131. – in Ukrainian.

[7] Volodymyr Zaslavsky, Eduard Nenakhov, and Anna Strizhak, "Commercial Bank's Credit Risk Optimization," *Teoriya optimalnykh reshenij* 4 (2005): 120–126. – in Russian.

[8] Heinz-Peter Berg, "Risk Management: Procedures, Methods and Experiences," *RT&A* no.2(17), vol. 1 (2010): 79–95.

[9] Andrii Kaminskyi, "Conceptual Approaches to Measuring Financial Risks," *Finansy Ukrainy* 5 (2006): 78–85. – in Ukrainian.

[10] Volodymyr Kravchenko, "Functional and Integral Approaches to Management of Entrepreneurial Risks: Theory and Practice," *Problemy systemnoho pidkhodu v ekonomitsi* 2(6) (2008), http://ecobio.nau.edu.ua/index.php/EPSAE/article/view/4012. – in Ukrainian.

[11] Volodymyr Zaslavsky, Anna Strizhak, "Credit Card Fraud Detection Using Self-Organizing Maps," *Information & Security: An International Journal* 18 (2006): 48–63, https://doi.org/10.11610/isij.1803.

[12] You Dai, Jin Yan, Xiaoxin Tang, Han Zhao and Minyi Guo, "Online Credit Card Fraud Detection: A Hybrid Framework with Big Data Technologies," *IEEE Trust Com-Big DataSE-ISPA*, no. 1 (2016): 1644–1651, https://doi.org/10.1109/TrustCom.2016.0253.

[13] K. Buryy, "Classification of Financial Risks of Banking Institutions," *Naukovyy visnyk Natsionalnoho universytetu bioresursiv i pryrodokorystuvannia Ukraïny*, no. 154(3) (2010): 49–56. – in Ukrainian.

[14] Saeed Nosratabadi, Gergo Pinter, Amir Mosavi and Sandor Semperger, "Sustainable Banking; Evaluation of the European Business Models," *Sustainability* 12, no. 6 (2020): 2314, https://doi.org/10.3390/su12062314.

[15] Amancei Cristian, "Practical Methods for Information Security Risk Management," *Informatica economica* 15, no. 1 (2011): 151–159, http://revistaie.ase.ro/content/57/13%20-%20Amancei.pdf.

[16] Mykhailo Zghurovskyi, “Scenario Analysis as a Systematic Prediction Methodology,” *Systemni doslidzhennia ta informatsiini tekhnolohii* 1 (2002): 7–38. – in Ukrainian.

[17] Solichul Huda, Riyanarto Sarno and Tohari Ahmad, “Increasing Accuracy of Process-based Fraud Detection Using a Behavior Model,” *International Journal of Software Engineering and its Applications* 10, no. 5 (2016): 175–185, https://doi.org/10.14257/ijseia.2016.10.5.16.

[18] Serhii Hlomazdin, “Choosing the Bank’s Credit Risk Assessment Methodology,” *Sotsium. Nauka. Kultura*, no.8 (2013). – in Ukrainian.

[19] David Hand and David Weston, “Statistical Techniques for Fraud Detection, Prevention, and Assessment,” *NATO Science for Peace and Security Series - D: Information and Communication Security. Mining Massive Data Sets for Security* 19 (2008): 257–270, https://doi.org/10.3233/978-1-58603-898-4-257.

[20] Volodymyr Shaporin and Olha Plachinda, “Development of Information Security Threat Models to Assess Harm for Assets,” *Technology audit and production reserves* 4, no. 2(24) (2015): 10–15, https://doi.org/10.15587/2312-8372.2015.47183. – in Russian.

[21] Hanna Krasovska, Olha Izmailova, and Kateryna Krasovska, “Prototyping of Intellectual Decision Support System for Organizational and Technological Trainings in Construction,” *Materials of the XII International scientific and practical conference, “Areas of scientific thought”. Mathematics. Physics. Modern Information technologies* 16 (Sheffield, UK: Science and Education, 2016), 101–105, http://journals.uran.ua/eejet/article/view/3881/3557.

[22] Hanna Krasovska, Olha Izmailova and Kateryna Krasovska, “Approach to Construct an Information Basis for Decision-Making System for a Comprehensive Assessment of Innovative Technogenic Safety Projects in Construction,” *Shliakhy pidvyshchennia efektyvnosti budivnytstva v umovakh formuvannia rynkovykh vidnosyn: Zb. naukovykh prats*, no.28 (2012): 222–229. – in Russian.

[23] Viktor Volkovich, Alexey Volochin, Vladimir Zaslavskyi and Igor Ushakov, “Models and Techniques for Reliability Optimization of Complex Systems,” (Kyiv: Naukova Dumka, 1993). – in Russian.

[24] Yurii Kozhedub, “Implementation of a Process Approach to Information Security Risk Management in Documents NIST P-ISSN 2411-1031,” *Information Technology and Security*, no.2(9) (2017): 76–89. – in Ukrainian.

[25] Oleksii Barybin, “Methodology of Testing for the Penetration of the Website of a Higher Education Institute,” *Standartyzatsiia, sertyfikatsiia, yakist. Systemy upravlinnia*, no.4(116) (2019): 12–18. – in Ukrainian.

[26] Oleksandr Korchenko, Svitlana Kazmirchuk, and Berik Akhmetov, *Applied Information Security Assessment Systems* (TsP Komprynt, 2017). – in Ukrainian.

[27] Sergey Klymov, "Methodology for Assessing Possible Damage from the Security Violation of the Information of the Automated System," *Yzvestyia TRTU*, no.4(33) (2003): 27–31. – in Russian.

[28] Yurii Medvedovskyi, "Modern Methods and Means of Analysing and Controlling the Risks of the CRAMM Company's System Security, RiskWatch in HRYF," 2004, www.ixbt.com/cm/informationsystem-risks012004.shtml. – in Russian.

[29] Dilek Bulbula, Hendrik Hakenes, and Claudia Lambert, "What Influences Banks' Choice of Credit Risk Management Practices," *Theory and Evidence* 40 (February 2019): 1–14, https://doi.org/10.1016/j.jfs.2018.11.002.

[30] Valeriy Dudykevych, Ivan Prokopyshyn, Vasyl Chekurin, Ivan Opirskyy, Yuriy Lakh, Taras Kret, Yevheniia Ivanchenko, and Ihor Ivanchenko, "A Multicriterial Analysis of the Efficiency of Conservative Information Security Systems," *Eastern-European Journal of Enterprise Technologies* 3, no. 9(99) (2019): 6–13. https://doi.org/10.15587/1729-4061.2019.166349.

[31] Thomas L. Saaty and Luis G. Vargas, *Decision Making with the Analytic Network Process: Economic, Political, Social and Technological Applications with Benefits, Opportunities, Costs and Risks* (Springer, 2013).

[32] Volodymyr Zaslavskyi, Kateryna Krasovska, and Maya Pasichna, "Application of the Method of Analysis of Hierarchies in Solving the Problem of Diversification of the Composition of the Portfolio of Electricity Generation," *Visnyk Kyivskoho universytetu, Seriia: Fizyko-matematychni nauky* 2 (2017): 123-131. – in Ukrainian.

[33] Olha Izmailova, Sofiia Pyda, Iryna Melnyk, and 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*, no.29 (2017): 109–118. – in Ukrainian.

About the Authors

Olha **Izmailova** is Candidate of technical sciences and Associate professor in the Department of Cyber Security and Computer Engineering in the Kiev National University of Construction and Architecture, Ukraine.
http://orcid.org/0000-0002-2905-1827

Hanna **Krasovska** is Candidate of technical sciences and Associate professor in the Department of Intelligent Technologies in the Taras Shevchenko National University of Kyiv, Ukraine. https://orcid.org/0000-0003-1986-6130

Kateryna **Krasovska** is PhD candidate in the Department of Mathematical Informatics in the Taras Shevchenko National University of Kyiv, Ukraine.
http://orcid.org/0000-0002-3468-8064

Volodymyr **Zaslavskyi** is Doctor of technical sciences and professor in the Department of Mathematical Informatics in the Taras Shevchenko National University of Kyiv, Ukraine. https://orcid.org/0000-0001-6225-1313