

THE DEVELOPMENT OF CORPORATE SECURITY IN THE CONTEXT OF COUNTERING THREATS TO DOING BUSINESS

Taras SHYRA ^{1*}, Kostiantyn SALYGA ², Vasyl DERII ³,
Igor PRYKHODKO ⁴, Svitlana SHYMKIV ⁵

¹*Faculty of Media Communications and Entrepreneurship, Ukrainian Academy of Printing, Lviv, Ukraine*

²*Department of Finance, Accounting and Taxation, Classic Private University, Zaporizhia, Ukraine*

³*Department of Accounting and Taxation, Ternopil National Economic University, Ternopil, Ukraine*

⁴*Department of Account, Taxation and Financial and Economic Safety,
Dnipro State Agrarian and Economic University, Dnipro, Ukraine*

⁵*Department of Insurance, Banking and Risk Management,
Kyiv Cooperative Institute of Business and Law, Kyiv, Ukraine*

Received 19 August 2020; accepted 27 May 2021

Abstract. The principal purpose of the study is to determine the main parameters of corporate security development in the enterprise in the context of determining the level of impact of external and internal threats. The study uses survey methods on the main internal and external threats that may affect the corporate security of enterprises. The purpose of the practical part of our study is to determine the level of these threats to corporate security.

The methodological basis of our study is the method of expert evaluation, which was conducted by interviewing people involved in the process of corporate security management of enterprises, as well as methods of the hierarchical organization using matrices of pair-wise comparisons. The major results of the study can be considered determining the hierarchy of influence of each of the threats affecting the corporate security of industrial enterprises, which will allow optimizing the security system and directing its activities to more pressing issues. Our method of the hierarchical organization of threats to corporate security does not take into account the specifics of the corporate security system of industrial enterprises in most European countries and now can be freely implemented mainly in industrial enterprises of Eastern Europe. The proposed method of assessing external and internal threats is currently optimized for the activities of industrial enterprises in Eastern Europe, including Ukraine and Poland. In the following, at an expansion of the given research, there is a possibility of introducing this methodology to the enterprises of other countries or other profiles. The relevance of this study lies in determining the level of threats that affect the corporate security of industrial enterprises. The methodology for assessing the level of influence of these threats is universal, therefore it can be used in the event of a change in the main threats, it is extremely relevant in the context of rapid globalization changes in the world.

Keywords: corporate security, parameters of the development, external and internal threats, risk, enterprise, matrix, the relationship graph.

JEL Classification: M14, G34, P42, L21.

Introduction

The priority of forming a methodological basis for ensuring corporate security of enterprises today is determined primarily by two key circumstances. Firstly, the need to create safe conditions for development for each business entity is determined by the riskiness of entrepreneurial activity in general and the difficult conditions for doing business in Ukraine due to the duration of transformation

processes and instability in the national economy. Secondly, the importance of the role of corporations functioning today, which they already play in the economic processes of our country and the growth of their influence, by analogy with other countries, in the future.

World experience convincingly proves that the activity of corporate structures contributes to the stabilization of the economic situation within a certain country, the

*Corresponding author. E-mail: education_univer21@yahoo.com

efficient use of available resources, and the satisfaction of the interests of the population.

The choice of a threat as an object of the focus of security subjects is not accidental, because, as was proved in the first chapter of the dissertation, next to risk, it is a form of danger. A decrease in security is the result of the negative impact of an internal or external threat. Risk cannot be ignored by security entities, but it is present in every decision that is made by the enterprise's managers (Nalla & Morash, 2002).

At the international level, the threat of increased competition in the European market and increased requirements for product quality, viewing environmental standards, and significant progress in updating production technology for industrial products using nanotechnologies and unlimited resources are relevant. The most significant threats to the national sublevel include, first of all, political and social instability, military operations on the territory of the country, the intensification of migration processes in the last few years, a decrease in the population and its solvency, a decrease in the technological level and a weakening of the scientific component in the production of industrial products, uncontrolled change of inflationary processes, etc. The regional level is largely determined by the economic parameters of the development of the region, geographical location, and other parameters.

Summarizing, it can be argued that assessing the dynamics and forecasting the impact of threats at all levels ensures the timely development and implementation of protective measures to optimize the necessary resource support (Halibozek et al., 2008). Given this, the driving factor for the development and improvement of all elements of corporate security should be the determination of the degree of influence of external and internal threats, which are decisive in the process of doing business.

Continuing the consideration of this aspect, it is worth noting that, with regard to threats on the microenvironment, security entities organize special studies and apply methods for obtaining and processing information that will be considered in the future, but at the macro level, it is sufficient to obtain data from open sources with clear tracking of key changes in the parameters of the development of world markets, the formation and filling of state and local budgets, individual government programs and strategies for the development of sectors of the national economy. The approach is also true when the threats of macro- and microlevels are examined in aggregate, but they determine different response priorities and also monitor the links between them, that is, they build a threat map and provide a systematic update of the parameters of such a model. The key is not only the creation of such a card, but the timely updating of information, since in a very short period of time a threat with a third priority level can go to the first level, and its implementation can entail significant losses for the enterprise. It is this aspect that underlies the methodological foundations of threat assessment, which

will be considered in the future on the basis of determining the essence of the following main stages (Zedner, 2003).

In order to see in more detail and clearly the level of influence of threats on the corporate security of industrial enterprises, in our work we used the method of pairwise comparisons for the hierarchical ordering of threats.

The main goal of the study is to form a specific model that demonstrated the influence of threats and the variability of defense mechanisms concerning certain group of threats, using mechanisms for the development of corporate security.

1. Analysis of recent research/Literature review

Domestic and foreign scientists paid a lot of attention to ensuring the safety of enterprises, in particular Abalkin (2019), Anilovska (2020), Sylkin et al. (2019a), Shtangret (2019), Szewczyk (2012), Yarochkin (2020), and others. Despite the scientific and practical significance of the work of these scientists, we note that some issues (Borodzicz & Gibson, 2006; Szewczyk, 2012) of a conceptual, methodological and methodological nature, in essence, the process of creating a corporate security system, the formation of mechanisms and the development and implementation of a strategy are not sufficiently explored. So, the need for improving the corporate security system through identification and identification of the main threats to its impact is being updated.

A theoretical study revealed that the issue of assessing threats to corporate attention is not given due attention. In a few publications, authors are limited to a list of possible threats (Berle & Means, 1997).

An important baseline in the assessment of threats is their consideration only in a separate range. Most scientific publications address threats that directly affect corporate security. This approach cannot be considered true enough, because, under such conditions, security actors in the majority can carry out operational or tactical measures. In our current view, it is necessary to expand the range of possible threats, that is, taking into account those that arise at the regional, national and international levels. They at some point in time may not have a direct impact on the corporate security of the enterprise, but in the medium or long term, they will become a source of threats that will be the focus of attention of security entities.

The issue of corporate security today is especially relevant and enjoys great interest among scientists from all over the world. In particular, one of those who most clearly and fully described the content, structure, and features of corporate security can be considered Ludbey et al. (2018).

Cabric (2017) studied the features of the existence and provision of corporate security at the level of commercial enterprises.

Another scholar who has studied the paradigm of corporate security and the possible threats that affect it

can be considered McKenzie-Skene (2019), Hardman (2018), and Frey et al. (2019).

The basis of this position was the hierarchical model of the external environment proposed by Shershneva and Oborskaya (2020), in which two levels are distinguished: the macroenvironment (international, national, regional) and the microenvironment. In the macro environment, three sublevels are determined by their totality of threats that are partially related, that is, they are scaled in a certain way. For example, the intensification of the financial crisis at the international sublevel causes negative changes in the national economy, in particular the external economic balance, and reduces the number of funds allocated to regional development programs, which in turn further provokes a decrease in demand for the products of this enterprise.

A broader vision of the essence of corporate security, as well as its main features, can be found in the scientific works of Cubbage and Brooks (2013), who studied the peculiarities of the existence of corporate security of the enterprise in the territory Asia-Pacific Region.

Stenning (2017) and Chapple (2014) were investigated the development of practical and theoretical achievements in the field of corporate security, in particular, focused on the participation and influence of international mechanisms of influence in this process.

Knight and Nurse (2020) examined the process of ensuring corporate security in the context of cybersecurity only, which made their work undeniably extremely valuable when considering external threats that affect the digital part of the enterprise, but at the same time they neutralized the importance of other types of threats.

With the development of the economy and the general globalization of mankind, scientists have come to realize the importance of improving existing methods of protection and ensuring corporate security, in particular in the context of the enterprise.

Briggs and Edwards (2006) and Wolf et al. (2007) in their work explored the adaptive mechanisms of corporate security to the current realities of today, including the state of the economy, levels and manifestations of existing risks, threats that affect the enterprise. The same opinion is shared by Roney (2014), who in his work emphasizes the importance of finding new approaches to corporate security, in particular at the enterprise level.

The idea of using the method of pairwise comparisons for the hierarchical ordering of threats is not new; it was used by a several scientists in solving important problems in the field of safety. In particular, Karaim (2016), to formulate the methodological foundations for crisis management in the economic security system of an enterprise, Kotlyarevsky et al. (2016), when modeling the impact of internal and external threats to the economic security of automobile enterprises, Zhyvko (2018) in determining the grounds for improving the system of economic security of enterprises.

It is advisable to note that at the moment in scientific research the pairing method has not been applied for

the hierarchical ordering of threats relative to corporate security (at least the author is not aware of this), therefore the material presented above is a definite step in deepening the formation of the methodological basis for ensuring corporate security and differs from existing developments today.

2. Methodology

2.1. The main stages of assessing the impact of threats on corporate security

First of all, it is worth noting the main stages of assessing the impact of threats on the corporate security of an enterprise (Figure 1).

In this figure, the main stages are systematized and detailed, it is intended to provide answers to the following questions:

- threats affect corporate security;
- how they can be ordered;
- which ones have the greatest impact.

Figure 1 is intended only to illustrate the general aspects of what actions should be taken to counter threats.

The basis of the first stage is high-quality information, which is generated in the system of accounting and analytical support of the enterprise and used by security entities to monitor external and internal threats. It needs to be clarified that this system forms a certain part of information about the external environment, in particular, the level of payment discipline of counterparties, the purchasing power of consumers, interaction with law enforcement and fiscal authorities, cooperation with local communities, etc.

The following list of the main objectives of monitoring threats to corporate security of enterprises can be defined:

- development of a system of indicators that contributed to a comprehensive assessment of the corporate security threats of a given enterprise based on the macro- and microlevels of its functioning environment and internal processes;
- assessing the potential impact of threats, tracking their dynamics;
- determination of losses from implementing the negative impact of external and internal threats;
- tracking information on the implementation by security entities of protective measures, that is, information support for implementing management decisions;
- assessing the effectiveness of implementing protective measures and the effectiveness of the actions of security entities.

The basis for the functioning of such a system should be the observance of the principle of continuity, that is, the systematic and timely receipt of the necessary quality information to monitor the presence and change of the influence of external and internal threats. This continuity is achieved by Sylkin et al. (2018):

- organization of a system of accounting and analytical support;

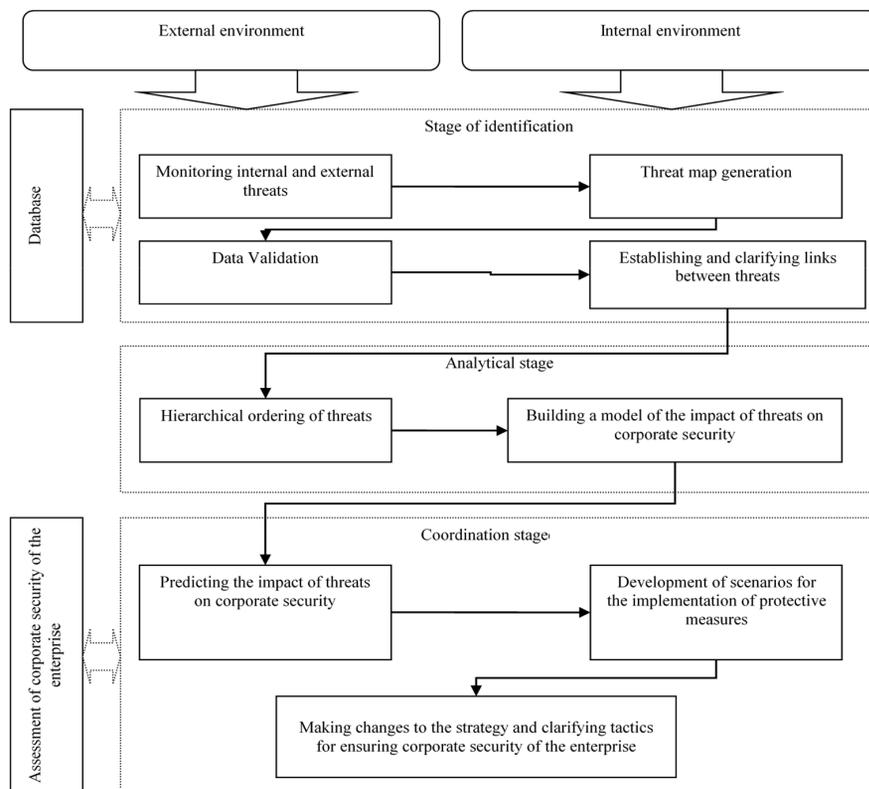


Figure 1. The main stages of assessing the impact of threats on corporate security (development by authors)

- the formation of a system for obtaining, systematizing, and presenting information necessary for security entities about changes in the internal and external functioning environment, which is not provided for by the accounting and analytical support system.

The information got on the results of monitoring requires systematization, which is advisable to use the created database on the influence of external and internal threats in the past and the effectiveness of the actions of security entities. The comparison allows tracking changes in the list of actual threats and creating a “threat map”. “Threat map” is a list of internal and external threats in the context of functional components. Comparing the current card with the previous option allows you to identify changes in the list of threats. The identification of changes is primarily the basis for checking the reliability of hourly information, clarifying factors that could lead to the emergence of an additional threat, or strengthening its influence on the corporate security of the enterprise. The same stage requires clarification of the links between threats. You can chew on the existence of vertical and horizontal bonds. The essence of the vertical ties we have considered above, arise between the threats of the macro (international, national, and regional) and the microlevel. On the horizontal side, they exist between threats within the corporate security of food reception according to its main functional components.

The analytical stage is a logical continuation of the previous one and consists of the hierarchical ordering of internal and external threats with the results presented in

the form of a model. Let us briefly consider the essence of this stage, starting with the justification of the need for a hierarchical ordering of threats. The reason is the fact that at the same time the attention of security entities to all threats is impossible. It is necessary to determine the totality that can lead to the most significant losses.

To implement this step, it is advisable to use the expert survey method. Threats that are important for security entities from a tactical and strategic point of view, for appropriate implementation of protective measures at different times, are subject to isolation. Hierarchical ordering can be carried out using the method of pairwise comparisons, which is based on a comparison of threats among themselves, followed by the construction of appropriate matrices and several mathematical calculations, which ultimately allows you to determine the priority levels of counteraction to key threats. It must be recognized that at the first stage of compilation when the matrices of pairwise threat comparisons are built, there is a subjective opinion of the executor about the relationship between them, the human factor is eliminated in the future due to the need to carry out a certain sequence of mathematical actions.

The third stage – the coordination one, being a continuation of the previous one, provides for the coordination of the results of modeling the impact of threats with the results of assessing corporate security. A low level of security with a certain functional component and the presence, or the increased influence of one or more threats, is the basis for the development and implementation of protective measures. In our opinion, achieving high efficiency in

ensuring corporate security is possible not only through an operational response but, above all, the development of tactics and strategy formation. Therefore, the third stage involves identifying all the basic circumstances and introducing the necessary changes in the tactics and strategy of ensuring corporate security of the enterprise.

2.2. Using an expert method to identify the key external and internal threats affecting corporate security of industrial enterprises

Within the framework of our research, it is quite difficult to implement all stages of the threat assessment, therefore we will focus on the individual, they will not allow us to fully take into account the peculiarities of the financial and economic activities of the enterprise, but they can be used by security entities as a guideline (Sylkin et al., 2019b). The stage of “formation and identification”, based on these circumstances, we carried out by applying the method of interviewing experts. For this, a cooperation plan was agreed by experts who are in the status of workers in industrial enterprises.

The group is represented by employees of enterprises of various types of economic activity; it allows, through generalization and agreement of opinions, to avoid subjectivity in assessing threats to corporate security. In addition, in the selection of experts, attention was also focused on the scale of activity of enterprises, which is represented by the number of employees.

Implementing the expert assessment method, we used the following selection criteria for experts:

- compliance with the principles of gender equality (in the survey accepted an equal number of women and men);
- at least 5 years of work experience in industrial enterprises;
- given that most experts are representatives of Ukrainian enterprises, in order to obtain clearer results, it was decided to attract representatives of industrial enterprises from other regions of Eastern Europe, in particular from Poland and the Czech Republic, into the structure of experts. Thus, 25% of the experts are representatives of industrial enterprises from Poland and the Czech Republic;
- 25% of representatives of experts have previously participated in scientific research and are familiar with the procedure of expert research;
- each expert passed the test of professionalism and reliability, which is described in detail below.

At the initial stages, the purpose of which was to select the most competent experts, in the framework of our study of professionalism and reliability, experts evaluated in the framework from 0 to 1. At first, the number of experts was 200 people, officially agreed to participate in the Expert Assessment and the processing of personal data. Subsequently, these 200 experts passed the test of professionalism and reliability, as a result of which a sample of the most competent was formed. This test

consisted of two parts: a general survey and an individual interview, during which professional skills and personal qualities were assessed. It is worth noting that, given the current unstable epidemiological situation in the world, all stages of the selection of experts were carried out remotely, the interview was conducted using the Skype and Zoom program.

The first stage, as already mentioned, consisted of 10 questions that directly related to the issue of ensuring corporate security at industrial enterprises. For example, one of the ten questions that the expert was asked was the following: Have you taken an active part in implementing activities related to the process of ensuring corporate security at your enterprise. If the experts are true (the value “true” means a positive answer regarding participation in the process of ensuring corporate security at the enterprise) answered 5 out of 10 questions, they received a total of 0.25 points, correctly answering 10 out of 10 questions, they received a dandy of 0.5 points. If they answered correctly on less than 5 questions, then they did not receive points and did not pass to the second stage of the test

The second stage of the test, as already mentioned, had the form of an interview, during which the main professional and personal qualities of experts were determined and evaluated. For this stage, experts could get up to 0.5 points.

As a result of passing the two-stage test, 80 of 200 experts received more than 0.7 points, which may indicate a high level of reliability and professionalism in the field of corporate security at the enterprise (Figure 2). It was this number of experts that was involved in identifying key internal and external threats that affect the corporate security of industrial enterprises.

Taking into account the opinions of experts working in enterprises with different numbers of employees is designed to ensure that threats to corporate security related to the human factor, the possibility of internal conflicts, etc. are taken into account. functional tasks related to corporate security (Figure 2).

The answers of the respondents allow us to conclude that despite the small share of enterprises where the security system is not properly organized (12.5%), the

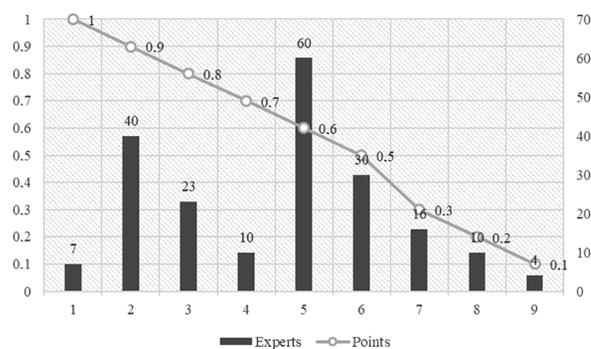
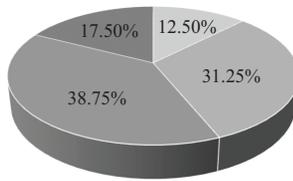
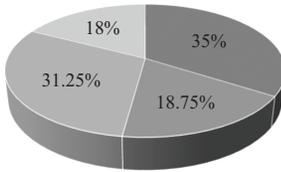


Figure 2. Professional and reliability test results (development by authors)



- Lack of an organized security system
- Actions aimed at suppressing theft and use of official position
- Priority of business development without control and current activities
- Countering threats and focusing on the efficient use of corporate resources

Figure 3. Accountability of internal processes in enterprises (development by authors)



- Not given due attention
- Operational measures are being taken to eliminate the consequences of the implementation of threats
- Corporate security is provided within the functional tasks of individual departments
- There is an established security system that can provide corporate security.

Figure 4. The ability to provide corporate security at the right level (development by authors)

attention of other security entities is focused on solving current problems, i.e. elimination of abuses and crimes by staff (Figure 3).

The last and most important in the context of our study was the question of the level of the general ability of enterprises to provide adequate corporate security (Figure 4).

According to the strategic vision of solving corporate security problems through forecasting and the timely application of protective measures, it is present only at individual enterprises. The reasons for this situation can be considered partial preservation of the security service as a unit responsible for protecting the property of the enterprise, as well as the lack of necessary experience in assessing external and internal threats, the lack of unnecessary resource support for organizing comprehensive protection.

2.3. Using software to implement the method of the hierarchical ordering of external and internal threats that affect corporate security

The main purpose of the use of this software in the research process is to conduct simulation (computer) modeling in system analysis by binary comparisons for subsequent hierarchical ordering.

The Borland Delphi 7 software environment was chosen to create the program. The source executable file of the mpp.exe pairwise comparison method takes up 608 kb of memory. The program is expected to be used in the Windows operating system environment.

The developed program can be used in research related to the analysis of process parameters for system design and for the multicriteria problem of the theory of decision-making by choosing an alternative.

In general, this program accords to the following algorithm:

Let a certain factor of the technological process be considered as a linguistic variable X , defined on a universal set U . To test X , we use the term S^* , which is defined by a fuzzy set in the form of a set of pairs:

$$S^* = \left\{ \frac{\mu_S(u_1)}{u_1}, \frac{\mu_S(u_2)}{u_2}, \dots, \frac{\mu_S(u_n)}{u_n} \right\},$$

where $u_i \in U$ is the universal set on which the fuzzy set is specified $u_i \in U$; $\mu_S(u_i)$ is the degree to which the element u_i belongs to a fuzzy set S^* .

It is necessary to determine the value $\mu_S(u_i)$ for all $i = \overline{1, n}$. The combination of these values will form a membership function.

The method that is proposed for solving the problem is based on the idea of distributing the degrees of membership of elements of a universal set under their ranks. The element number u_i is taken to be the number $rs(u_i)$ characterizing the importance (or weight) of the element in the property's formation, which is described by the fuzzy term S . The degree of membership $\mu_S(u_i)$ of the elements $u_i \in U$ by the fuzzy term S is calculated by relative rank estimates $\frac{r_i}{r_j} = a_{ij}$ ($i, j = \overline{1, n}$), which form the matrix of pairwise comparisons A .

The program implementation of these actions is as follows. In the beginning, the number n is the dimension of the term S . Next, the task of relative estimates of the ranks of the element u_i for the first row of the matrix of pair-wise comparisons is performed. Again, based on the properties of the specified matrix, the relative estimates of the ranks for the next rows are completed and the values of the membership function $\mu_S(u_i)$ are calculated. When you click on the button to build a graph in a separate window, a graph of the membership function for the term S is built.

3. Results of the research

3.1. Identification of key external and internal threats affecting corporate security of industrial enterprises

Based on the results of a survey of experts, we selected eight threats, in relation to which the opinions of experts were the most similar and provided additional notation, they will be used in the process of hierarchical ordering (Figure 5). For further ease of use, threat names have been abbreviated.

In the process of comparing two threats, a scale of the relative importance of objects from 1 to 9 is used (Figure 5). The information basis for the application of the

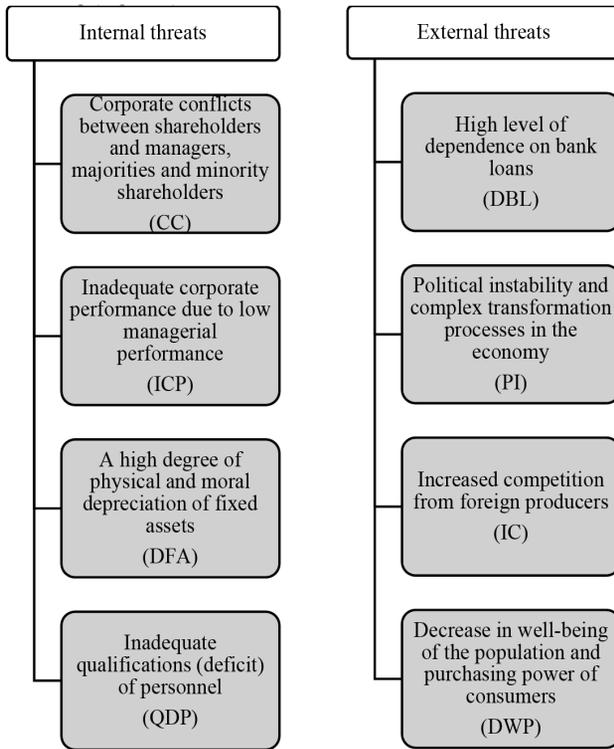


Figure 5. The list of key threats to corporate security of industrial enterprises (development by authors)

pair comparison method is the key threats obtained by applying an expert survey (Figure 4), based on which the matrix of pair comparisons is built (Table 1).

Table 1. Matrix of paired comparisons of key threats to corporate security of industrial enterprises (development by authors)

	CC	ICP	DFA	QDP	DBL	PI	IC	DWP
1	2	3	4	5	6	7	8	9
CC	1	1	3	2	4	6	5	7
ICP	1	1	2	5	3	1	4	6
DFA	1/3	1/2	1	3	1	1	2	4
QDP	1/2	1/5	1/3	1	1/2	1/4	1	1
DBL	1/4	1/3	1	2	1	1/2	1	3
PI	1/6	1	1	4	2	1	3	5
IC	1/5	1/4	1/2	1	1	1/3	1	2
DWP	1/7	1/6	1/4	1	1/3	1/5	1/2	1

Using the software of the methodology of paired comparisons and the corresponding specialized literature (Gileta et al., 2012), we determined the sums of the elements of the columns of the matrix of paired comparisons.

The purpose of the proposed program is to conduct simulation (computer) modelling in system analysis using the binary comparison method. To study the technological process, it is important to single out a combination of factors in it, characterise it and establish the weight of the influence of each of them. Assessment of the advantages of

one factor over another is obtained using expert judgment. Often, due to the presence of numerous factors of various nature, it is difficult for an expert to assess each of them. Therefore, two factors are compared in pairs with each other and give preference to one or the other (Table 2).

Table 2. The sum of the column elements of the matrix of paired comparisons of key threats to the corporate security of industrial enterprises (development by authors)

Z_i	CC	ICP	DFA	QDP	DBL	PI	IC	DWP
S_j	0.287	0.225	0.117	0.049	0.083	0.143	0.059	0.034

The purpose of the proposed program is to carry out simulation (computer) modeling in system analysis by the method of binary comparisons. For the study of the technological process, it is important to distinguish a set of factors in it, it is characterized and the establishment of the weight of the influence of each of them. An assessment of the advantage of one factor over another is obtained using expert judgment. Often, due to the presence of a large number of factors of various nature, it is difficult for an expert to give a real assessment to each of them. Therefore, two factors are compared in pairs and give preference to one or the other. This method allows comparing two factors with each other and expressing the comparison result in a rank scale. When there are more than two factors, then using this method compare each pair of factors and get a series of comparison results. The result is written into a matrix of pair-wise comparisons, each element of which establishes the advantage of one factor over another. An important property of a matrix is its consistency. For the degree of consistency of the matrices of pairwise comparisons, the concordance ratio is used. The consistency ratio is required to be less than one-tenth. When the condition is not met, the expert is advised to revise his judgments and edit the matrix of pair-wise comparisons. To implement the simulation process by the method of paired comparisons, an interface has been developed (Figure 6), where all intermediate parameters of the simulation are displayed.

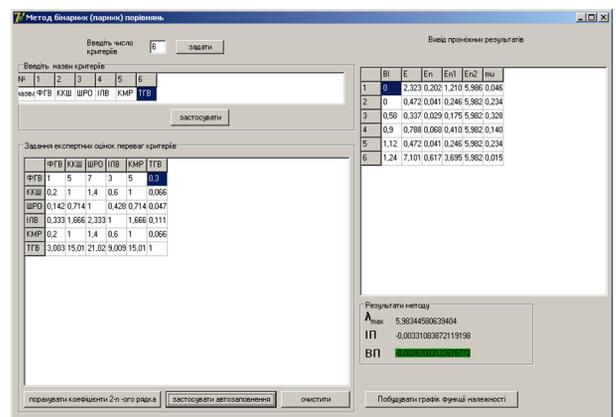


Figure 6. Binary comparison analysis program interface (development by authors)

First, the number of process criteria is entered. After pressing the “set” button, we proceed to the stage of setting the mnemonic names of the criteria. Next, we turn to the assignment of expert assessments of advantages in the matrix of pair-wise comparisons. The introduction of expert assessments of the advantages of the criteria is necessary only for the 1st line. Next comes the modelling stage. It consists in achieving the required value (less than one-tenth) of the consistency ratio. If the desired value of the consistency relation has not been achieved, the experts’ judgments about the advantages of the criteria are revised.

Using this computer program made it possible for us to understand the degree of influence of each of the threats to the corporate security of an industrial enterprise and to place them at the appropriate levels (Figure 7).

3.2. Forming a graph of the relationship between threats to corporate security of industrial enterprises

According to the results of the calculations it was determined that the consistency index of the matrix of pair-wise comparisons is within the normal range (≤ 0.1), that is, we have satisfactory comparison results. The results obtained (Table 2) make it possible to prioritise the impact of selected threats on the corporate security of industrial enterprises (Figure 7).

The results obtained indicate that the threat “The presence of corporate conflicts between shareholders and managers, majorities and minorities” is at the highest level. Accordingly, this particular threat requires special attention on the part of security actors – in the next section we will present a mechanism for countering corporate security threats.

A similar situation exists with respect to the following levels: if the actions of security entities should include the identification of threats related to insufficient competence, corporate corruption and abuse of managerial positions, then with respect to political instability and transformational changes in the national economy, only timely adaptation is possible, which should be preceded by forecasting

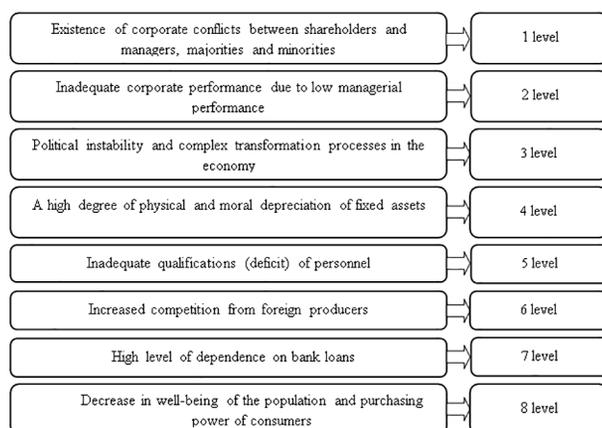


Figure 7. Graph of relationships between threats to corporate security of industrial enterprises (development by authors)

and developing possible scenarios.

In graphical form, we have shown the possibility of implementing protective measures against a specific group of threats that can be defined as “internal” by applying mechanisms and developing a corporate culture, which will be paid attention to in the following sections of the dissertation. Along with this, it is also determined that in relation to a group of “external” threats, the priority negative impact of which requires an appropriate reaction of the security entities of the enterprise, it is advisable to carry out in cooperation with external security entities. Such cooperation will not allow eliminating the threat, but the information received, consultations, support and coordinated interaction can reduce the possible negative consequences.

4. Discussion and interpretation of results obtained

The results obtained form the basis for improving the process of ensuring corporate security by developing appropriate mechanisms and developing a corporate culture. Based on the proven impact of threats on the level of corporate security, the content of the main stages of assessing the impact of threats (identification and identification, analytical and coordination) is considered, the implementation of which, using the expert survey method, determined the group of key threats by applying graph theory, were hierarchically ordered by the degree to which protective measures are necessary.

The result of a fruitful analysis is the formation of a model on the reflective highlighted through the calculations of threats and their impact. Running through the entire analysis, the process of achieving Figure 8 is as follows: an analysis of the enterprise operating environment is carried out; specialized experts are involved; expert assessment is carried out; highlights the key external and internal threats; the comparison of the selected threats with the use of software is carried out; according to the results of the comparison of the definition of the hierarchy of their influence; the model is formed is presented in Figure 8, which acts as information support for making decisions on ensuring corporate security at the enterprise.

Determined hierarchical ordering is the result of the analytical stage of assessing the impact of threats on the corporate security of industrial enterprises. The main components of the next stage is a model that characterizes not only the results to be evaluated, but also the implemented protective measures in accordance with their essence of threats (Figure 8).

The model we have developed allows us not only to understand the levels of impact and the hierarchy of existing threats that have an impact on the corporate security of industrial enterprises but also to form effective mechanisms to counter these threats.

Summarising, it is worthwhile to emphasise once again that the coordination of the results of the corporate security

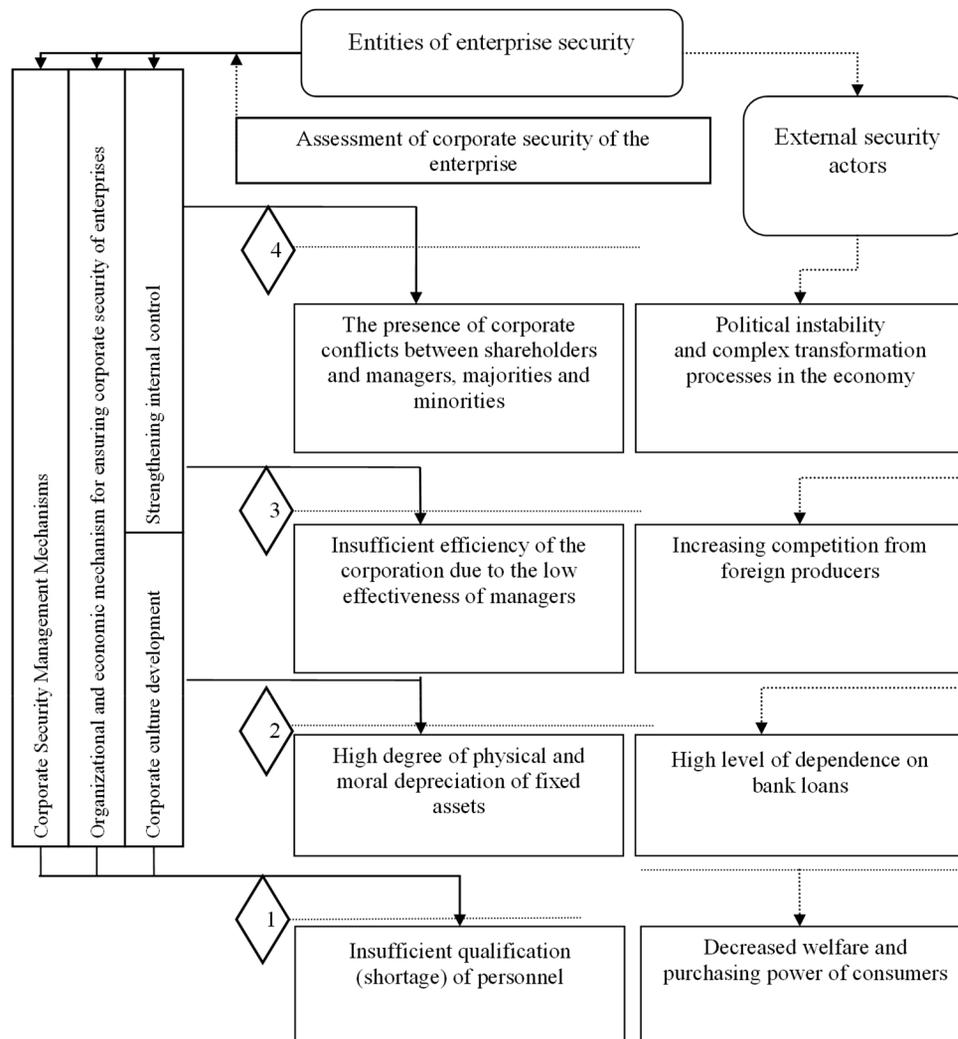


Figure 8. Threat impact model and protection options (development by authors)

and threats assessment forms the necessary informational ground not only for implementing protective measures but also for changing the company’s activities to increase the efficiency of its financial and economic activities and adapt it in accordance with the dynamics of processes in the field of the implementation.

The results of the hierarchical ordering of key external and internal threats indicate that the threat “The presence of corporate conflicts between shareholders and managers, majorities and minority shareholders” is at the highest level. It is concluded that this particular threat requires special attention from security actors. In graphical form, by constructing a model of the influence of threats and protection options, the possibility of implementing protective measures against a certain group of “internal” threats by using mechanisms and developing a corporate culture has been demonstrated.

It is worth noting that, according to the authors, the formed model has a significant practically managerial significance, it consists in providing a real opportunity for companies to independently assess the level of corporate security and in a timely manner to make management

decisions necessary for the survival and prosperity of the company. In turn, if we talk about the theoretical significance of the study, then this model can become a powerful basic one for further research of corporate security threats.

Conclusions

Based on the results of the study, the article considered the main parameters of the development of corporate security of enterprises in the context of determining the level and countering external and internal threats.

In the study, we proposed to use a methodological approach that forms a clear idea not only about the level of corporate security, that is, fixing the situation at a certain point in time, but thanks to the definition and characterization of the impact of threats – the possibility of applying not only operational protective measures but also tactical and strategic ones. That is, we are talking about reducing uncertainty, forming an information basis for predicting changes in corporate security and matching the effective use of the resources provided by security entities.

Based on the proven impact of threats on the level of corporate security, the content of the main stages of assessing the impact of threats is examined, the implementation of which, using the expert survey method.

The results of a hierarchical streamlining of key external and internal threats indicate that the threat “The presence of corporate conflicts between shareholders and managers, majorities and minority shareholders” is at the highest level. It is concluded that this particular threat requires special attention from security actors. In graphical form, by constructing a model of the influence of threats and protection options, the possibility of implementing protective measures against a certain group of “internal” threats, by applying mechanisms and developing a corporate culture.

This model is the final stage of the study, which will allow to fully graphically depict the level of impact of threats on the corporate security of an enterprise, while simultaneously depicting possible protection measures against these threats.

Funding

All studies, the results of which are presented in this article, were carried out by the authors on their own at their own expense.

Disclosure statement

Authors declare that they have no competing financial, professional, or personal interests from other parties.

Author contributions

The authors contributed equally.

References

- Abalkin, L. (2019). Economic security: threats and their reflection. *Economic Issues*, 12, 4–13.
- Anilovska, G. (2020). Calls to the army of competitors in the field of competition and market. *Science Newsletter NLTU of Ukraine*, 23(1), 177–182.
- Berle, A. A., & Means, G. C. (1997). *The modern corporation and private*. The MacMillan Company.
- Borodzicz, E. P., & Gibson, S. D. (2006). Corporate security education: towards meeting the challenge. *Security Journal*, 19(3), 180–195. <https://doi.org/10.1057/palgrave.sj.8350016>
- Briggs, R., & Edwards, C. (2006). *The business of resilience: corporate security for the 21st century*. Demos.
- Cabric, M. (2017). *From corporate security to commercial force: a business leader's guide to security economics*. Butterworth-Heinemann, Linacre House. <https://doi.org/10.1016/B978-0-12-805149-8.00002-9>
- Chapple, L. (2014). Corporate governance and securities class actions. *Australian Journal of Management*, 39(4), 525–547. <https://doi.org/10.1177/0312896213512320>
- Cubbage, C., & Brooks, D. J. (2013). *Corporate security in the Asia-Pacific Region*. CRC Press.
- Frey, R., Rosler, L., & Lu, D. (2019). Corporate security prices in structural credit risk models with incomplete information. *Mathematical Finance*, 29(1), 84–116. <https://doi.org/10.1111/mafi.12176>
- Gileta, I. V., Senkivsky, V. M., & Melnikov, O. V. (2012). *Simulation in system analysis by binary comparison method: Computer program: registration certificate author*. Rights to the work 41832 Ukraine № 42107, application 17.11.2011, publ. 02.07.2012, Bull. 27.
- Halibozek, E., Jones, A., & Kovacich, G. L. (2008). *The corporate security professional's handbook on terrorism*. Elsevier.
- Hardman, J. (2018). Three steps forward, two steps back: a view from corporate security practice of the moveable transactions (Scotland) bill. *Edinburgh Law Review*, 22(2), 266–273. <https://doi.org/10.3366/elr.2018.0485>
- Karaim, M. M. (2016). *Anti-crisis technologies in the management of economic security of the enterprise*. A. M. Stangret (Ed.). Ukrainian Academy of Printing.
- Knight, R., & Nurse, J. (2020). A framework for effective corporate communication after cyber security incidents. *Computers & Security*, 99. <https://doi.org/10.1016/j.cose.2020.102036>
- Kotlyarevsky, Ya. V., Melnikov, O. V., Shtangret, A. M., & Ratushnyak, Yu. V. (2016). Hierarchical ordering of factors that hinder or stimulate the development of the information sphere in Ukraine. *Scientific and Practical*, 2(75), 39–52.
- Ludbey, C. R., Brooks, D. J., & Coole, M. P. (2018). Corporate security: identifying and understanding the levels of security work in an organisation. *Asian Journal of Criminology*, 13, 109–128. <https://doi.org/10.1007/s11417-017-9261-x>
- McKenzie-Skene, D. (2019). A practical guide to granting corporate security in Scotland. *Edinburgh Law Review*, 2, 284–285. <https://doi.org/10.3366/elr.2019.0559>
- Nalla, M., & Morash, M. (2002). Assessing the scope of corporate security: common practices and relationships with other business functions. *Security Journal*, 12(1), 7–19. <https://doi.org/10.1057/palgrave.sj.8340119>
- Roney, M. (2014). Corporate security requires an integrated approach. *Forbes*, 5, 58.
- Shershneva, Z. E., & Oborskaya, S. V. (2020). *Strategic management [a textbook]*. Kyiv Publishing House.
- Shtangret, A. (2019, 22 September). Corporate security: theoretically ambush a medical care in Ukraine. In *Practices of approaches to creative management of economic processes: by X International science-practical conference*, Vol. 1 (pp. 38–39). National Agriculture University.
- Stenning, P. (2017). Corporate security in the 21st century: theory and practice in international perspective: Book Review. *Policing and Society*, 27(2), 248–250. <https://doi.org/10.1080/10439463.2016.1266146>
- Sylkin, O., Kryshchanovych, M., Zachepa, A., Bilous, S., & Krasenko, A. (2019a). Modeling the process of applying anti-crisis management in the system of ensuring financial security of the enterprise. *Business: Theory and Practice*, 20, 446–455. <https://doi.org/10.3846/btp.2019.41>
- Sylkin, O., Krystyniak, M., Pushak, Y., Ogirko, O., & Ratushnyak, Y. (2019b). Anti-crisis strategy in the system of ensuring financial security of the engineering enterprise: theoretical and practical aspects. In *2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T)* (pp. 256–260). Kyiv, Ukraine. <https://doi.org/10.1109/PICST47496.2019.9061346>
- Sylkin, O., Shtangret, A., Ogirko, O., Melnikov, A. (2018). Assessing the financial security of the engineering enterprises as

- preconditions of application of anti-crisis management: practical aspect. *Business and Economic Horizons*, 14(4), 926–940. <https://doi.org/10.15208/beh.2018.63>
- Szewczyk, S. (2012). The intra-industry transfer of information inferred from announcements of corporate security offerings. *The Journal of Finance*, 47(5), 1935–1945. <https://doi.org/10.1111/j.1540-6261.1992.tb04689.x>
- Wolf, K. D., Deitelhoff, N., & Engert, S. (2007). Corporate security responsibility: Towards a conceptual framework for a comparative research agenda. *Cooperation and Conflict*, 42(3), 294–320. <https://doi.org/10.1177/0010836707079934>
- Yarochkin, V. (2020). *Securitology – the science of life safety*. Axis-89.
- Zedner, L. (2003). Too much security. *International Journal of the Sociology of Law*, 31(3), 155–184. <https://doi.org/10.1016/j.ijsl.2003.09.002>
- Zhyvko, Z. B. (2012). *Economic security of the enterprise: essence, mechanism of maintenance and management* [monograph]. Liga-Press.