

# BUSINESS RISK MANAGEMENT TECHNIQUES AND EXPERT METHODS OF THEIR EVALUATION

©2020 SHEVCHUK I. B., STARUKH A. I., VASKIV O. M.

UDC 330.131.7:004

JEL: D81

## Shevchuk I. B., Starukh A. I., Vaskiv O. M. Business Risk Management Techniques and Expert Methods of their Evaluation

The article is aimed at researching the problem of risk when substantiating decisions not only of a strategic nature, but also at the stage of short-term planning. In this regard, the problem of risk assessment takes on an independent theoretical and applied value as an important part of the theory and practice of the system of information security management. The next step was to review, research and analyze the system of business planning management for an economic entity that relates to a complex IT system. One of the options for solving this issue may be the development and creation of a computer expert system of business planning. The research results are the types and categories of business risks being analyzed, as well as the impact of IT risks in business, in particular, techniques of business risk management are disclosed. The risk management methodologies such as CRAMM, COBIT, FRAP and OCTAVE, which are among the main and widely used in both government and commercial organizations around the world, have also been described. The methodologies under research have both positive and negative aspects in risk management, and do not provide for the resolution of the consequences of risks that have not been minimized or prevented. Studies have shown that as methods of economic and mathematical modeling of the solution to the task of optimizing the management of business planning processes is proposed to use the results of works on the study and use of artificial intelligence methods, namely, technologies for the development and creation of computer expert systems to implement information support and support managerial decisions. Prospects for further research in this direction are our proposed development of an expert system as an instrumentarium of the system of business process management and support of managerial decision-making, as well as the use of such expert systems to assess risks by business entities, which will provide them with an efficient instrumentarium of forming business plans for the implementation of various production and commercial projects.

**Keywords:** risk, business risks, business processes, methodology, management, expert methods.

**DOI:**

**Fig.:** 13. **Tabl.:** 1. **Formulae:** 1. **Bibl.:** 24.

**Shevchuk Iryna B.** – D. Sc. (Economics), Associate Professor, Head of the Department of Digital Economics and Business Analytics, Ivan Franko National University of Lviv (1 Universytetska Str., Lviv, 79001, Ukraine)

**E-mail:** ibshevchuk@ukr.net

**ORCID:** <https://orcid.org/0000-0003-4386-3730>

**Starukh Anna I.** – PhD (Economics), Associate Professor, Associate Professor of the Department of Digital Economics and Business Analytics, Ivan Franko National University of Lviv (1 Universytetska Str., Lviv, 79001, Ukraine)

**E-mail:** anniyta.star@gmail.com

**ORCID:** <https://orsid.org/0000-0003-3282-1746>

**Researcher ID:** <http://www.researcherid.com/H-1671-2019>

**Vaskiv Oksana M.** – Senior Lecturer of the Department of Digital Economics and Business Analytics, Ivan Franko National University of Lviv (1 Universytetska Str., Lviv, 79001, Ukraine)

**E-mail:** omvaskiv@ukr.net

**ORCID:** <https://orcid.org/0000-0001-8312-2828>

УДК 330.131.7:004

JEL: D81

## Шевчук І. Б., Старух А. І., Васків О. М. Технології управління бізнес-ризиками та експертні методи їх оцінки

Мета статті полягає в дослідженні проблеми ризику при обґрунтуванні рішень не тільки стратегічного характеру, але і на стадії коротко-строгового планування. У зв'язку з цим проблема оцінки ризиків набуває самостійне теоретичне і прикладне значення як важлива складова частина теорії та практики системи управління інформаційною безпекою. Наступним кроком було розглянути, дослідити та зробити аналіз системи управління бізнес-проектів для господарюючого суб'єкта, який відноситься до складної ІТ-системи. Одним із варіантів рішення даного питання може стати розробка та створення комп'ютерної експертної системи бізнес-планування. У результаті дослідження проаналізовано види та категорії бізнес-ризиків, а також вплив ІТ-ризиків у бізнесі, зокрема розкрито технології управління бізнес-ризиками. Також здійснено опис методик управління ризиками, таких як CRAMM, COBIT, FRAP та OCTAVE, котрі є одними із основних і широкоживаних як в урядових, так і в комерційних організаціях по всьому світу. Досліджувані методики мають як позитивні, так і негативні сторони в управлінні ризиками, а також не передбачають розв'язку наслідків ризиків, які не вдалося мінімізувати або їм запобігти. Дослідження показали, що як методи економіко-математичного моделювання рішення задачі оптимізації управління процесами бізнес-планування пропонується використовувати результати робіт по вивченню та використанню методів штучного інтелекту, а саме: технології розробки та створення комп'ютерних експертних систем для реалізації інформаційного забезпечення та підтримки прийняття управлінських рішень. Перспективами подальших досліджень у даному напрямі є запропонована нами розробка експертної системи як інструментарію системи управління бізнес-процесами та підтримки прийняття управлінських рішень, а також використання таких експертних систем для оцінки ризиків суб'єктами господарювання, що забезпечить їм ефективний інструментарій формування бізнес-планів для реалізації різних виробничих і комерційних проектів.

**Ключові слова:** ризик, бізнес-ризик, бізнес-процеси, методика, управління, експертні методи.

**Рис.:** 13. **Табл.:** 1. **Формул:** 1. **Бібл.:** 24.

**Шевчук Ірина Богданівна** – доктор економічних наук, доцент, завідувачка кафедри цифрової економіки та бізнес-аналітики, Львівський національний університет імені Івана Франка (вул. Університетська, 1, Львів, 79001, Україна)

**E-mail:** ibshevchuk@ukr.net

**ORCID:** <https://orcid.org/0000-0003-4386-3730>

**Старух Анна Ігорівна** – кандидат економічних наук, доцент, доцент кафедри цифрової економіки та бізнес-аналітики, Львівський національний університет імені Івана Франка (вул. Університетська, 1, Львів, 79001, Україна)

*E-mail:* anniyta.star@gmail.com

*ORCID:* <https://orcid.org/0000-0003-3282-1746>

*Researcher ID:* <http://www.researcherid.com/H-1671-2019>

**Васьків Оксана Миколаївна** – старший викладач кафедри цифрової економіки та бізнес-аналітики, Львівський національний університет імені Івана Франка (вул. Університетська, 1, Львів, 79001, Україна)

*E-mail:* omvaskiv@ukr.net

*ORCID:* <https://orcid.org/0000-0001-8312-2828>

УДК 330.131.7:004

JEL: D81

**Шевчук І. Б., Старух А. И., Васьків О. Н. Технологии управления бизнес-рисками и экспертные методы их оценки**

Цель статьи заключается в исследовании проблемы риска при обосновании решений не только стратегического характера, но и на стадии краткосрочного планирования. В связи с этим проблема оценки рисков приобретает самостоятельное теоретическое и прикладное значение как важная составная часть теории и практики системы управления информационной безопасностью. Следующим шагом было рассмотреть, исследовать и сделать анализ системы управления бизнес-проектированием для хозяйствующего субъекта, который относится к сложной ИТ-системе. Одним из вариантов решения данного вопроса может стать разработка и создание компьютерной экспертной системы бизнес-планирования. В результате исследования проанализированы виды и категории бизнес-рисков, а также влияние ИТ-рисков в бизнесе, в частности раскрыты технологии управления бизнес-рисками. Также осуществлено описание таких методик управления рисками, как CRAMM, COBIT, FRAP и OCTAVE, являющихся одними из основных и широко используемых как в правительственных, так и в коммерческих организациях по всему миру. Исследуемые методики имеют как положительные, так и отрицательные стороны в управлении рисками, а также не предусматривают разрешение последствий рисков, которые не удалось минимизировать или предотвратить. Исследования показали, что в качестве методов экономико-математического моделирования решения задачи оптимизации управления процессами бизнес-планирования предлагается использовать результаты работ по изучению и использованию методов искусственного интеллекта, а именно: технологии разработки и создания компьютерных экспертных систем для реализации информационного обеспечения и поддержки принятия управленческих решений. Перспективами дальнейших исследований в данном направлении является предложенная нами разработка экспертной системы как инструментария системы управления бизнес-процессами и поддержки принятия управленческих решений, а также использование таких экспертных систем для оценки рисков субъектами хозяйствования, что обеспечит им эффективный инструментарий формирования бизнес-планов для реализации различных производственных и коммерческих проектов.

**Ключевые слова:** риск, бизнес-риски, бизнес-процессы, методика, управления, экспертные методы.

**Рис.:** 13. **Табл.:** 1. **Формул.:** 1. **Библ.:** 24.

**Шевчук Ирина Богдановна** – доктор экономических наук, доцент, заведующая кафедрой цифровой экономики и бизнес-аналитики, Львовский национальный университет имени Ивана Франко (ул. Университетская, 1, Львов, 79001, Украина)

*E-mail:* ibshevchuk@ukr.net

*ORCID:* <https://orcid.org/0000-0003-4386-3730>

**Старух Анна Игоревна** – кандидат экономических наук, доцент, доцент кафедры цифровой экономики и бизнес-аналитики, Львовский национальный университет имени Ивана Франко (ул. Университетская, 1, Львов, 79001, Украина)

*E-mail:* anniyta.star@gmail.com

*ORCID:* <https://orcid.org/0000-0003-3282-1746>

*Researcher ID:* <http://www.researcherid.com/H-1671-2019>

**Васьків Оксана Николаївна** – старший преподаватель кафедры цифровой экономики и бизнес-аналитики, Львовский национальный университет имени Ивана Франко (ул. Университетская, 1, Львов, 79001, Украина)

*E-mail:* omvaskiv@ukr.net

*ORCID:* <https://orcid.org/0000-0001-8312-2828>

Nowadays, IT plays an important, sometimes crucial, role in all human activities, including business. Thus, not only business risks but also IT risks, as an integral part of them, should be taken into consideration. When developing strategies and plans aimed to minimize business risks, one should focus on peculiarities of a certain business enterprise or business process and the degree of impact of information technologies on them.

In view of the above, we argue that when managing business risks, it should be understood that their main source is IT risks.

Therefore, an important factor in improving the level of information security is using mathematical methods and models in the preparation of decisions to assess risks and their possible prevention. However, the use of

these methods in solving various problems is often impossible due to their complexity. Thus, expert methods of risk assessment have become more widespread.

Under the current instability of the economy, developing and creating an expert system for implementing business planning processes based on the use of modern information technologies will help conduct marketing research for industry or service production, draft a financial plan, and provide risk management and assessment effectively.

Problems related to business risk management techniques and expert methods of their assessment were analyzed in works of a number of Ukrainian and foreign scientists including R. Voronko [1], A. Pastoev [11], K. Korotnev [12], A. Alekseev [15], A. Shorikov [18], V. Krisevich [19], D. Rutkovskaya [20], and others.

They highlight the importance of studying types and categories of business risks as well as the impact of IT risks in business, in particular, describe IT risk management techniques and expert methods for assessing them.

Acknowledging the works of above mention scientists, it should be noted that this problem has not been currently solved, and the development of an expert system as a tool for business process and decision support management is a prospect for further research.

The *aim* of the article is to identify business risk management techniques and the expert methods of their assessment.

It is safe to assert that we live in a century where technologies are determining the future. Anyone involved in real-time business knows how important technologies are to business. In the initial stages of development, business was fully dependent on the workforce, but with the development of technologies, business tries to keep pace with them. For every business, technologies are important for enhancing its efficiency and achieving success. Since technologies have inherent importance in business, business risks include IT risks.

Considering entrepreneurial risks, we can say that there is no single view of risks and their correlation (or identity) with business risks [1].

Business risk is a risk of inadequate profit or even loss associated with uncertainty — increasing competition, customer preferences, strikes, changes in the government policy, etc. Business risk arises from competition, market conditions, assortment of goods, etc.

The two risks that lead to business risk are:

1. *Internal risk*, which arises within an organization. These risks are manageable. They are caused by such factors as strikes, work stoppages, factory accidents, employee negligence, machine malfunction, technological obsolescence, damage of goods, fire outbreaks, etc.;

2. *External risk*, which arises from outside the company and, therefore, is not controllable. It can be caused by fluctuations of prices, changes in customer tastes or government norms, force majeure, etc. [2; 3].

After considering and studying business processes, the structure of business risks can be presented as follows (Fig. 1) [4; 6].

IT risk is a threat to business data, critical systems, and business processes. It is related to such aspects as usage, ownership, operation, involvement of IT in an organization. IT risks can harm a company, decreasing its value; they often result from incorrect process and event management [7].

The investigation of IT risks makes it possible to divide them into three categories (Fig. 2): 1) personnel risks (these include managing access to resources, granting it in strict accordance with the functions performed by the employee and monitoring the use of resources; 2) risks associated with failure or malfunction of the equipment; 2) risks of using illegal software [8].

As was already mentioned, IT risks are a source of business risk and cover a number of important business areas shown in Fig. 3 [7].

Any change in the information infrastructure has a direct or indirect impact on all aspects of enterprise activity and, in fact, this complicates the analysis of the IT implementation effectiveness since it is very difficult to distinguish the impact of information technologies on the functioning of a company as a separate variable, and it is difficult to cover all areas of the impact of the IT used [9].

Risk management strategy is the art of managing enterprise activity under uncertainty, based on risk prediction and risk mitigation techniques.

As for the risk management system, it consists of two subsystems: the object of management and the subject of management (Fig. 4).

The *object of management* is the risk, risky investment and economic relations between entities in the process of entrepreneurship.

The *subject of management* is a special group of people that ensures purposeful operation of the management object, using different techniques and methods of managerial influence [10].

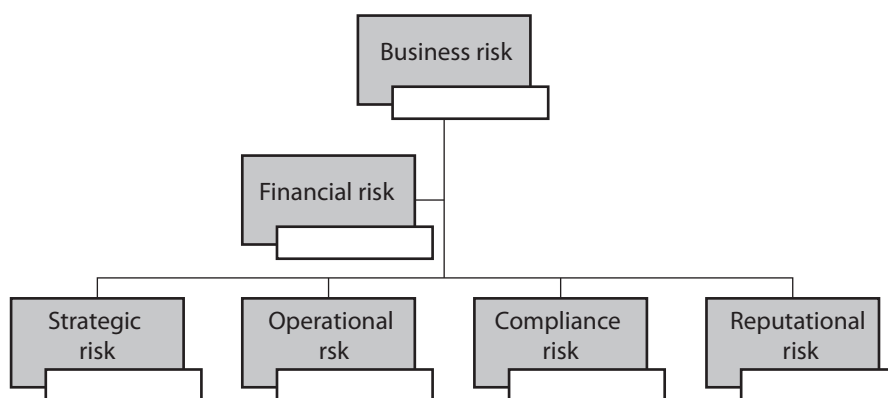
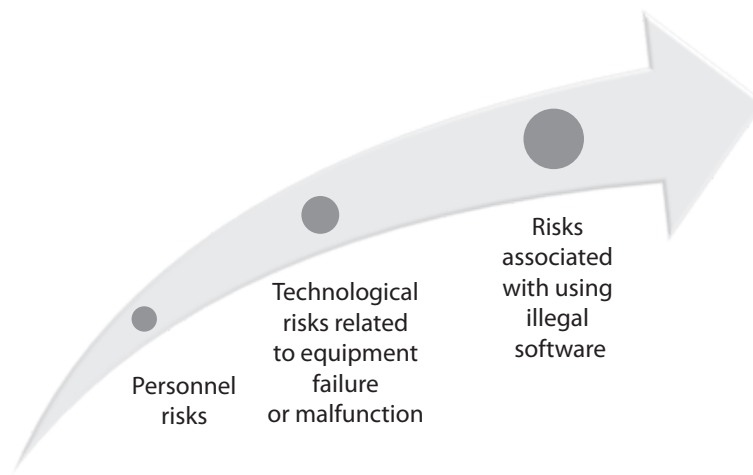


Fig. 1. Types of business risks



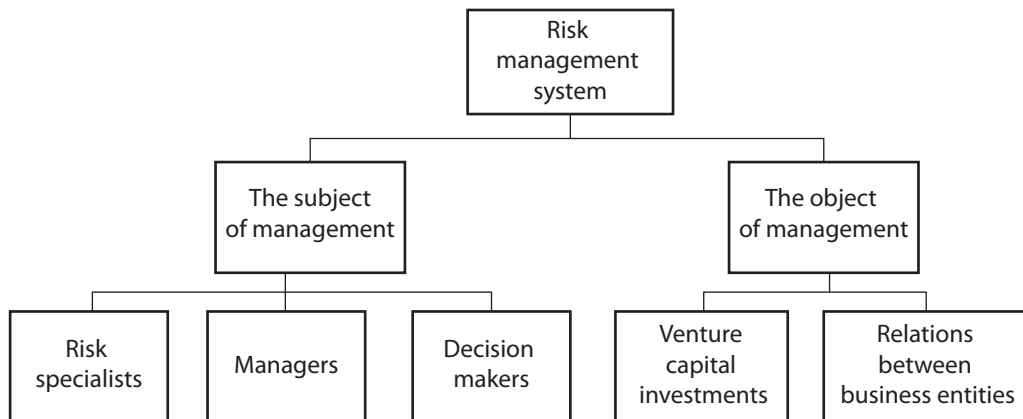
**Fig. 2. Categories of business risks**

Source: developed by the author based on [8].

| Accessibility   | Productivity   | Security  | Responsibility              |
|---|--|---|-----------------------------|
| inability to access the IT systems required for business operations | reduced productivity due to delayed access to the IT systems | compromised business data as a result of unauthorized access or use | violation of laws and rules |

**Fig. 3. IT risks in business**

Source: developed by the author based on [7].



**Fig. 4. Risk management subsystems**

Source: developed by the author based on [10].

For successful management of risky business situations, one should follow the basic principles of risk management (Fig. 5) [10].

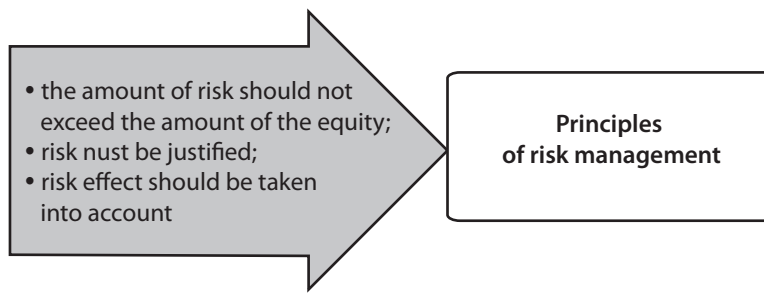
The most common IT risk management techniques in the world are CRAMM, COBIT for Risk, FRAP, OCTAVE; they have both certain advantages and limitations [11–13].

The CRAMM method (CCTA Risk Analysis and Management Method) is based on information security management standards and describes the correlation between vulnerable IT assets and the threats that may af-

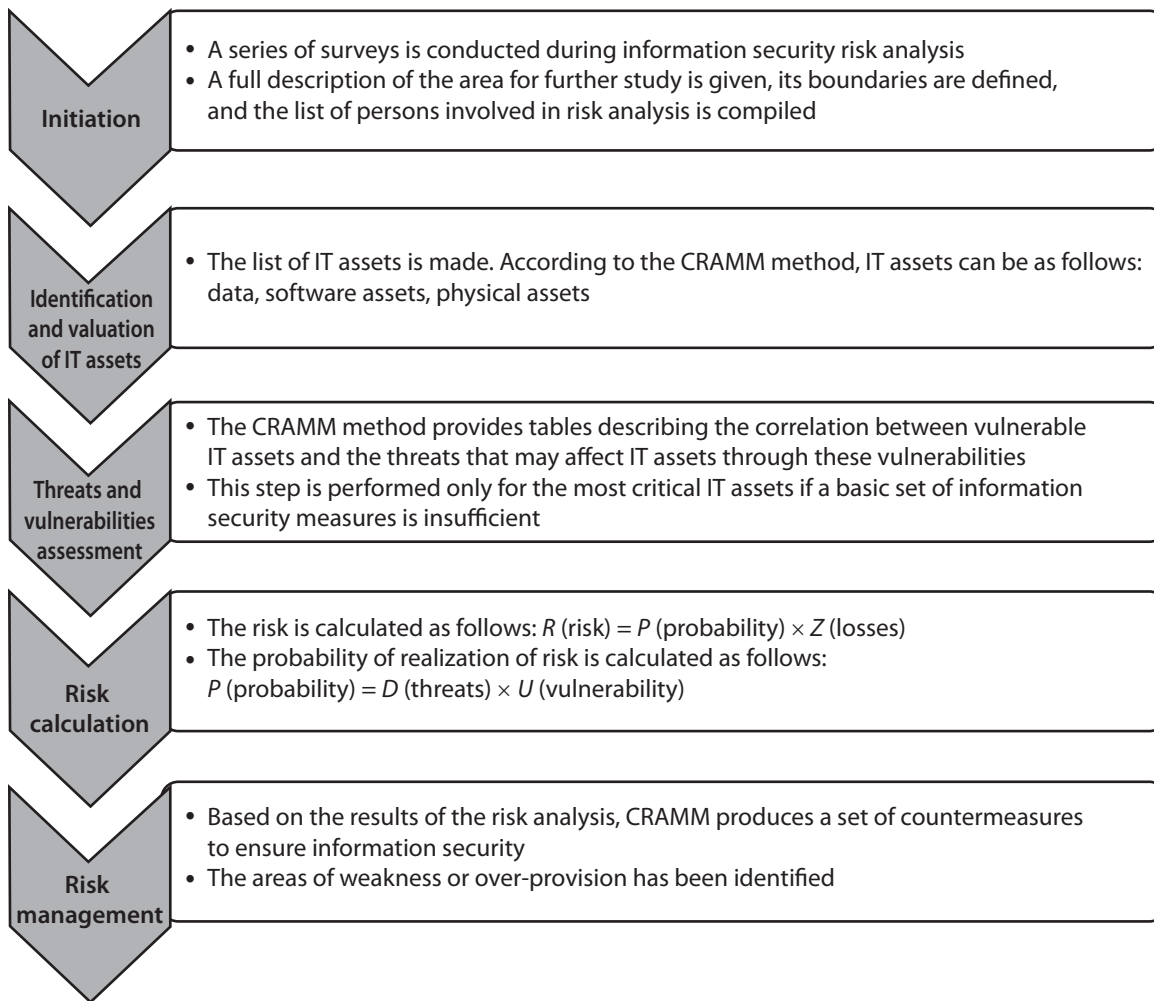
fect IT assets through these vulnerabilities. The process of risk management according to the CRAMM method consists of the following stages (Fig. 6) [5; 12–16].

The COBIT methodology, in implementing the function and process of managing IT risks in an organization, singles out the following components that have a significant impact on the risks and their management (Fig. 7) [5; 12; 13].

The Facilitated Risk Analysis Process (FRAP) describes an approach to qualitative risk evaluation. The purpose of the methodology is to identify, evaluate and



**Fig. 5. Basic principles of risk management**



**Fig. 6. CRAMM Stages**

record the composition of information on risks security for a pre-defined field of study.

For the analysis and evaluation of information security, a project team is created; the results of the brainstorming carried out by the project team during the risk analysis and evaluation session are presented in the Fig. 8 [12; 13; 16].

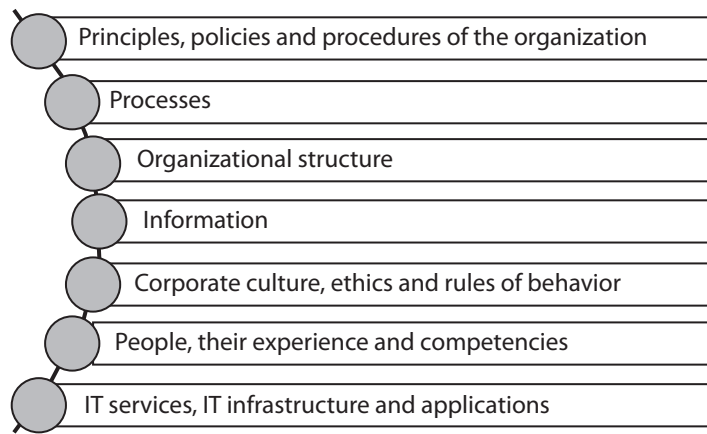
OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) describes an approach to qualitative risk assessment. The current version of this framework is OCTAVE Allegro. This methodology is in-

tended to formalize and optimize the evaluation of information security risks and provide the possibility for obtaining the necessary for the organization results with minimal time and resources.

According to OCTAVE Allegro, the IT risk management process consists of the following steps (Fig. 9) [12; 13; 17]:

Some advantages and disadvantages of the described methodologies are given in Tbl. 1.

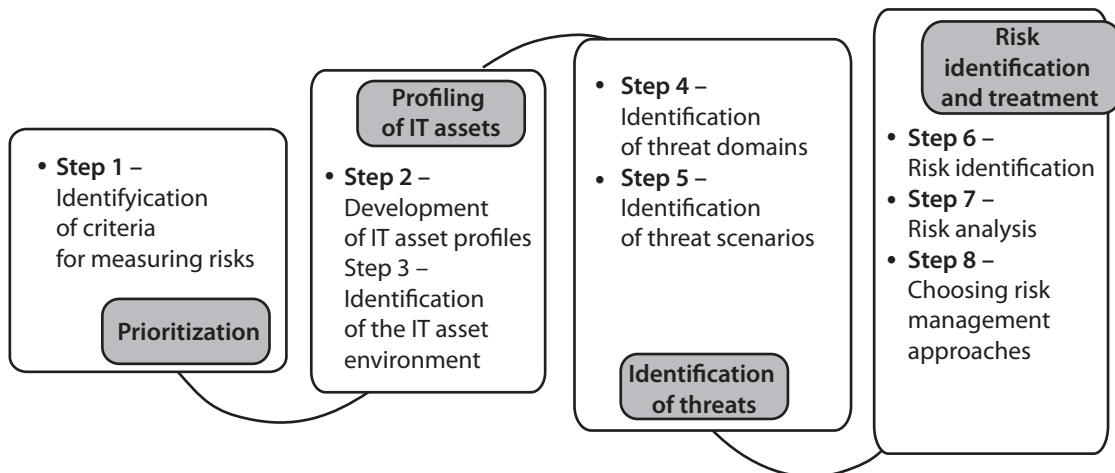
The approaches to risk management may vary, depending on the methodology used for risk analysis and management; all of them contain a detailed description



**Fig. 7. Main components of COBIT**

| The result of the brainstorming during the risk analysis and evaluation session |                                      |                             |   |
|---|--------------------------------------|-----------------------------|---|
| Vulnerability of the analyzed objects   | Potential threats to confidentiality | Integrity and accessibility | Probability of these threats and losses they cause to the core activities of the organization |

**Fig. 8. The result of the brainstorming during the risk analysis and evaluation session**



**Fig. 9. The risk management process according to OCTAVE Allegro methodology**

Source: developed by the author based on [12; 13; 17].

of the instructions for the implementation of each of the listed risk management stages as well as recommendations for choosing the best methodology, depending on the specifics of the organization.

In the modern economy, business planning is an integral part of the functioning of any economic entity, and a modern system for managing business process is a tool required for its successful operation. A project management system for an economic entity is a complex IT system developed on the basis of a relevant economic and mathematical model. The design and creation of an

expert system for business planning can be a solution to this problem.

We propose to use the results of research on artificial intelligence, namely the technology of developing and creating expert systems to provide information and decision support as methods of economic and mathematical modeling to optimize the management of business planning processes.

Under the current economic instability, the development and creation of an expert system for the implementation of business planning processes, based on the use of modern information technologies, can be an ef-

Advantages and disadvantages of risk management techniques

| Technique | Advantages   | Disadvantages  |
|-----------|--|--|
| CRAMM     | <ul style="list-style-type: none"> <li>– a pure formalized description of the methodology that minimizes the possibility of errors in the implementation of risk analysis and management processes;</li> <li>– the availability of risk analysis automation tools minimizes the time and effort spent on risk analysis and management activities</li> </ul>  | <ul style="list-style-type: none"> <li>– high complexity of collecting raw data;</li> <li>– high consumption of resources and time to implement IT risk analysis and management processes</li> </ul>   |
| COBIT     | <ul style="list-style-type: none"> <li>– relationship with the COBIT shared library;</li> <li>– repeatedly tested method;</li> <li>– a clear formalized description of the methodology</li> </ul>  | <ul style="list-style-type: none"> <li>– involvement of a large number of stakeholders;</li> <li>– lack of the ability to measure risks in monetary terms</li> </ul>   |
| FRAP      | <ul style="list-style-type: none"> <li>– simplicity and transparency of the process;</li> <li>– lowest labor costs for performing risk analysis and assessment;</li> <li>– involvement of a small number of participants ensures that communication costs within the project team are minimized and results are coordinated with all stakeholders</li> </ul> | <ul style="list-style-type: none"> <li>– absence of a well-regulated risk management process and detailed supporting materials, such as catalogs of threats, vulnerabilities, etc.;</li> <li>– absence of a deep decomposition, detailed and accurate risk assessment</li> </ul> |
| OCTAVE    | <ul style="list-style-type: none"> <li>– an iterative approach provides a gradual increase in the risk analysis profundity;</li> <li>– low labor costs for performing risk analysis and assessment</li> </ul>  | <ul style="list-style-type: none"> <li>– lack of detailed supporting materials;</li> <li>– lack of ability to measure risks in monetary terms</li> </ul>   |

fective toolkit to support an economic entity's decision-making when choosing a specific business project that meets the set goals [18].

To formalize knowledge in expert systems, certain rules should be used; these rules establish relationships between data and facts to derive logical conclusions ("cognitive results") similar to those used by a person in solving similar problems.

It should be noted that the main advantage of expert systems designed to provide information and management decision-making support is the possibility to carry out training and accumulate knowledge in the system in the process of their operation, i.e. to accumulate formalized information, which is used in the following processes of logical inference.

In general, an expert system used in business consists of the database (data in different formats, structured according to the architecture of the system), knowledge base (the part of the system that contains facts and knowledge from the relevant subject area, structured and formalized using various methods), output subsystem, problem solver (software implementation of the mechanism for forming the results of solving sub-tasks and a certain task as a whole, based on algorithms connected with the database, including the initial data, and the knowledge base), knowledge acquisition subsystem, explanation subsystem, subsystem of training and intelligent user interface [19].

Fig. 10 shows the structure of an expert system for business planning containing the main subsystems described above.

Such an expert system is an intelligent system for providing information and decision support in business planning that is intended for business entities in various sectors of the economy.

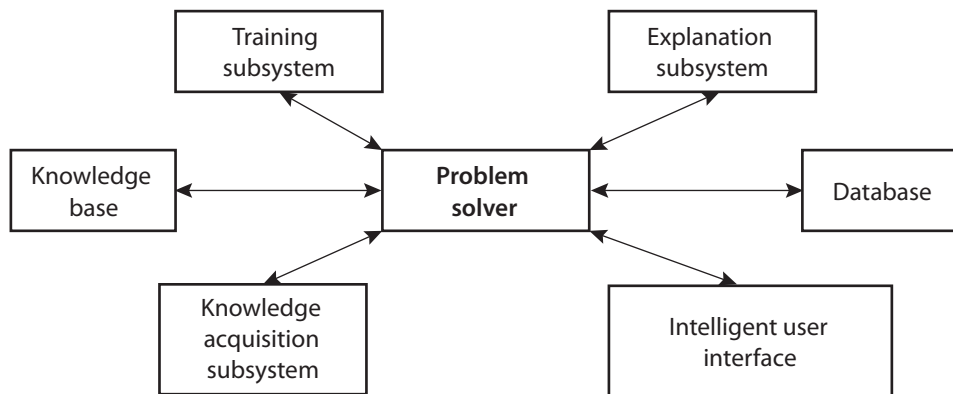
Expert systems have been successfully used in those areas where, in addition to the application of standard algorithmic methods based on accurate calculations, there is a need for specific analytical experts' knowledge and experience, and decision making is formed under incomplete data and depends on qualitative rather than quantitative estimates [20].

These subject areas include, first of all, the area of financial activity analysis, where the effectiveness of the made decisions depends on comparing many different factors, accounting complex cause and effect relationships, applying non-trivial logical considerations, etc. Thus, many companies operating on the New York Stock Exchange employ expert systems for making decisions in many industries (Fig. 11).

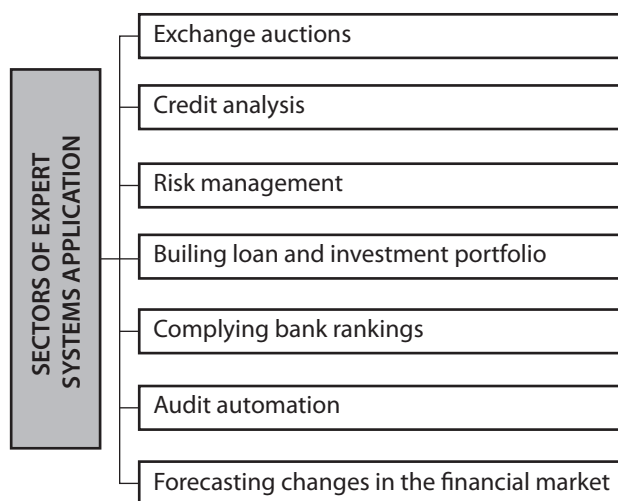
The use of such expert systems by economic entities will allow them to have an effective toolkit for forming business plans to implement various production and commercial projects, taking into account business risks.

Widely used expert methods are the methods of expert evaluation that are conducted by a group of experts under conditions of uncertainty or risk. Expert methods can be divided into three subgroups [22], which are presented in Fig. 12.

The methods that are most commonly used in risk management are the method for expert evaluation, rank-

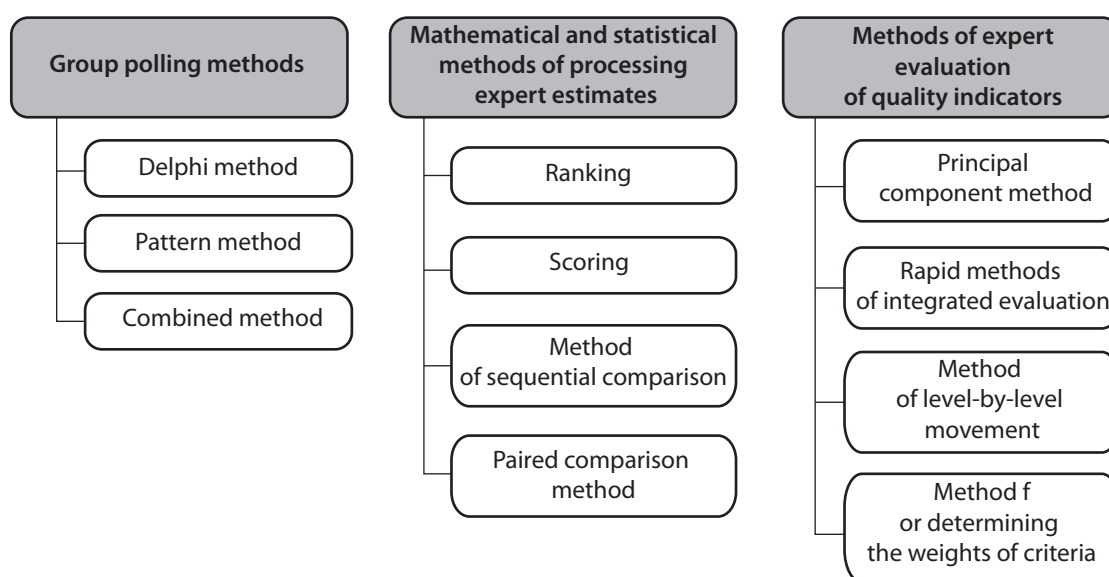


**Fig. 10. Structure of an expert system for business planning**



**Fig. 11. Sectors of expert systems application**

Source: developed by the author based on [21].



**Fig. 12. Classification of expert methods**

Source: developed by the author based on [22].



ing, the Delphi method, the paired comparison method and scoring.

The method of expert evaluation usually implies processing the opinions of experienced experts (qualified professionals). That is, this method involves collecting and studying estimates of probability of losses by different specialists based on their own intuition, knowledge and experience. These estimates are made with consideration for all risk factors as well as statistics.

The implementation of the method of expert evaluation is much more complicated if the number of evaluation indicators is small. The basic requirements for expert analysis are presented in Fig. 13.

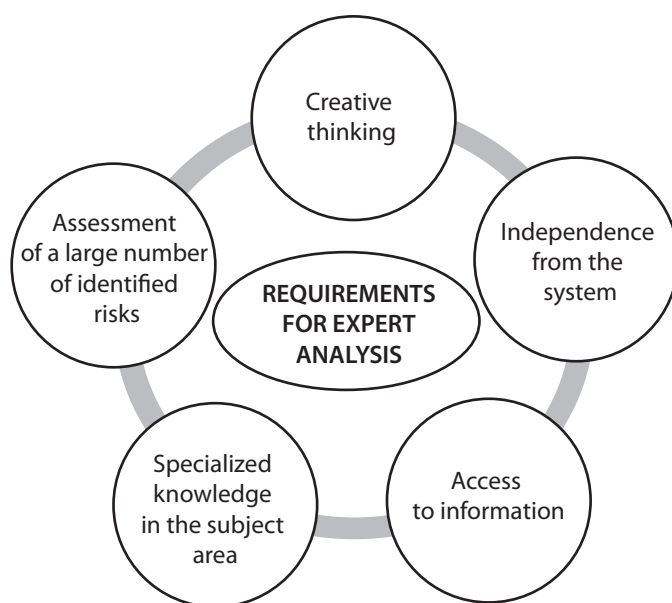


Fig. 13. Basic requirements for expert analysis

This method is often applied in developing modern information security management systems as well as in forecasting and long-term planning.

To provide conditions for improving quality and effectiveness of expert evaluation, active and persistent involvement of professionals at each stage (phase) of decision-making is required.

The stage-by-stage risk assessment approach is based primarily on identifying risks for each stage of the project separately, and then the overall result across the project is summarized [23].

Different methods are used to obtain the final result (expert assessments), the most common of them are questionnaires and the methods of group expertise. That is, each expert, working individually, is provided with a list of primary risks based on questionnaires about all stages of the project and is asked to evaluate the probability of the risks in accordance with the following rating system:

- ✦ 0 – the risk is considered insignificant;
- ✦ 25 – low risk probability;

- ✦ 50 – nothing certain can be said about the occurrence of the risk;
- ✦ 75 – high risk probability;
- ✦ 100 – the risk is certain to occur.

Expert estimates are analyzed for consistency according to certain rules. First, the maximum permissible difference between estimates of two experts on any factor should not exceed 50. Second, comparisons are made in absolute values (no plus or minus sign is taken into account). This eliminates unacceptable differences in experts' estimates of the probability of a separate risk. If the number of experts is three or more, then the estimates are compared in pairs.

As a rule, two experts are chosen to assess the consistency of the experts' opinions across the risk set. The basic rule is the maximum divergence of opinions of these experts (minimum cohesion). To calculate the discrepancy, the absolute values of estimates are summarized and the result is divided by the number of simple risks. The result obtained should not exceed 25.

In case of any contradictions between the experts' opinions (at least one of the above mentioned rules is not fulfilled), they are discussed at the experts' meeting. If contradictions are absent, all the expert's estimates are reduced to the average value (arithmetic mean) and used in the subsequent calculations.

There are other methods of expert risk assessment. One of them is the *ranking method*. The algorithm of its implementation is as follows.

At the first stage of information processing, all the estimates should be arranged in descending order.

Next, the average value of all estimates is calculated by the formula of the arithmetic mean.

The obtained values are divided into four equal intervals.

In case if evaluations of experts fall into extreme intervals, these experts are asked to justify their opinions. Other experts become familiar with their justification (under complete confidentiality).

The following rounds of discussion take into account those factors that were accidentally lost by the experts in the first round of the survey. As a result, in the second round, there is a less divergence of opinions.

*Delphi method* involves the rejection of direct communication between experts in the research process. Thus, the essence of this method lies in the individual interviewing of all members of the group through questionnaires in order to clarify their opinions based on personal experience and knowledge about future hypothetical events [24].

*Risk scoring* is a risk expertise based on a summarizing indicator, which is determined using a number of private indicators (factors) of the risk degree assessed by experts. The following steps are expected:

- ✦ selection of the factors directly affecting the risk degree of the project;
- ✦ outlining a generalized criterion and individual indicators characterizing each factor;
- ✦ assessment of this criterion in terms of risk degree;
- ✦ development of risk management recommendations.

Obviously, the high quality of expertise is achieved in the case of high consistency of experts' opinions of several factors. However, when using any method of expert evaluation, there is a problem associated with inaccuracy of the results obtained due to such factors as: poor choice of specialists, dominance of opinion (usually that of "authoritative leader"), etc. Therefore, it is necessary to carry out an expertise on the reliability of the obtained estimates.

One of evaluation indicators is Kendall's coefficient of concordance (rank correlation coefficient), which is calculated as follows:

$$W = \frac{12S}{m^2(n^3 - n)}, \quad (1)$$

where  $m$  – is the number of experts in the group;

$n$  – is the number of factors studied;

$S$  – is the sum of squared rank differences (deviations from the mean value).

The results of the analysis are within the following limits:

- ✦  $W < 0.2-0.4$  – concordance among the experts is low;
- ✦  $W > 0.6-0.8$  – concordance among the experts is high;
- ✦  $W = 1$  – the opinions of all experts are concordant.

Thus, it can be concluded that expert evaluation of risks is a very effective and simple method for analyzing occurrence of adverse events, especially in the area of information security management systems. Moreover, due to its simple organization, this method allows to cover a wide range of investigated factors.

However, due to the exceptional subjectivity of experts' responses, it is necessary to adhere to certain rules in conducting the expertise as well as to analyze the degree of concordance of experts' opinions in order to identify the quality of this expertise.

## CONCLUSIONS

Consequently, considering IT risks in business processes, we can argue that IT risks are the main source of business risks since the basic processes of an enterprise are performed using information technologies. Minimization of the risks and assurance of maximum information security demands IT risk management based on the enterprise's specifics.

In the research, techniques of IT risks management were described. We took a closer look at CRAMM, COBIT, FRAP and OCTAVE techniques, which are widely used by government and business organizations all around the world. The studied techniques have both advantages and disadvantages for managing risk and do not provide solution for eliminating the consequences of the risks that were not minimized or prevented.

The article suggests the application of expert systems in solving problems of risk evaluation that are difficult for a human expert. In most cases, expert systems are effective for tasks that are difficult to formalize or do not have an algorithmic solution.

Therefore, we can conclude that when developing an expert system, information support and optimization of business planning processes are implemented. In turn, the use of such expert systems for assessing risks by economic entities will allow them to have effective tools to form business plans for the implementation of various production and commercial projects. ■

## LITERATURE

1. Воронко Р. М. Оцінка та контроль бізнес-ризиків суб'єктів господарювання споживчої кооперації України. *Вісник Національного університету «Львівська політехніка»*. Серія «Менеджмент та підприємництво в Україні: етапи становлення і проблеми розвитку». 2017. № 862. С. 40–48. URL: [http://ena.lp.edu.ua:8080/bitstream/ntb/41599/2/2017n862\\_Voronko\\_R\\_M-Evaluation\\_and\\_monitoring\\_40-48.pdf](http://ena.lp.edu.ua:8080/bitstream/ntb/41599/2/2017n862_Voronko_R_M-Evaluation_and_monitoring_40-48.pdf)
2. Єсєєва І. В., Москаленко В. О. Основні види ризиків та їх вплив на конкурентоспроможність молокопереробних підприємств. *Економіка і організація управління*. 2014. № 3–4. С. 80–87. URL: <http://jeou.donnu.edu.ua/article/view/1092/1110>
3. Гожий О., Кобилінський І., Лугінець Д. Підхід до оцінювання ризиків у задачах планування. *Вісник На-*

- ціонального університету «Львівська політехніка». Серія «Комп'ютерні науки та інформаційні технології». 2014. № 800. С. 98–105. URL: <http://ena.lp.edu.ua:8080/bitstream/ntb/25926/1/16-98-105.pdf>
4. Business Risk: вебсайт. URL: <https://businessjargons.com/businessrisk.html?fbclid=IwAR0BhV81y0fe0V0JIEekCXgq0XjJK5ekWrycGn96R-zT-azxE7S82PeQVXY>
  5. Васьків О. М., Шевчук Ю. І. IT-ризиків як основне джерело бізнес-ризиків. *Polish Journal of Science*. 2019. Nr. 20. S. 28–36.
  6. Васьків О. М., Шевчук Ю. І. IT-ризиків та їх зв'язок з бізнес-ризиками // *The Modern Economic Research: Theory, Methodology, Practice: Conference Proceedings : II International Scientific Conference (September, 27)*. 2019. Kielce, Poland : Baltija Publishing. 156 p. S. 78–82.
  7. What board members need to know – and do. Information technology risks in financial services. URL: <https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-ccg-information-technology-risk-in-fs.pdf>
  8. Сингина А. А. Взгляд на управление рисками информационных систем. *Молодой ученый*. 2011. № 6. Т. 1. С. 101–105. URL: <https://moluch.ru/archive/29/3284>
  9. Песоцкая Е. Ю. Необходимость управления рисками в области информационных технологий. *Современные проблемы науки и образования*. 2007. № 6. Ч. 3. С. 48–52. URL: <http://www.science-education.ru/article/view?id=821>
  10. Ткаченко В. Сучасні підходи до оцінки ризиків інформаційних технологій. Управління ризиками IT / Active Audit Agency. 2010. URL: <https://ppt-online.org/172211>
  11. Пастоев А. Методологии управления IT-рисками. *Открытые системы СУБД*. 2006. № 08. URL: <https://www.osp.ru/os/2006/08/3584582/>
  12. Коротнев К. Методики управления рисками информационной безопасности и их оценки (ч. 1). 14.05.2018. URL: <https://safe-surf.ru/specialists/article/5193/587932/>
  13. Коротнев К. Методики управления рисками информационной безопасности и их оценки (ч. 2). 22.05.2018. URL: <https://safe-surf.ru/specialists/article/5194/587935/>
  14. Управление IT рисками. 20.02.2018. URL: <https://www.itexpert.ru/rus/newsline/articles/detail.php?ID=8936>.
  15. Алексеев А. Управление рисками. Метод CRAMM / ЗАО «ИТ Эксперт». 2010. URL: [https://www.itexpert.ru/rus/ITEMS/ITEMS\\_CRAMM.pdf](https://www.itexpert.ru/rus/ITEMS/ITEMS_CRAMM.pdf)
  16. Аникин И. В. Метод оценки рисков для уязвимостей информационных систем, основанный на нечеткой логике. *Информация и безопасность*. 2014. Т. 17. № 3. С. 468–471.
  17. Аникин И. В., Емалетдинова Л. Ю., Кирпичников А. П. Методы оценки и управления рисками информационной безопасности в корпоративных информационных сетях. *Вестник технологического университета*. 2015. Т. 18. № 6. С. 195–197. URL: <https://cyberleninka.ru/article/v/metody-otsenki-i-upravleniya-riskami-informatsionnoy-bezopasnosti-v-korporativnyh-informatsionnyh-setyah/viewer>
  18. Шориков А. Ф., Буценко Е. В. Экспертная система инвестиционного проектирования. *Прикладная информатика*. 2013. № 5. С. 96–103.
  19. Экспертные системы для персональных компьютеров: методы, средства, реализации: справ. пособие / Кричевич В. С., Кузьмич Л. А., Шиф А. М. и др. Минск: Выш. шк., 1990. 197 с.
  20. Рутковская Д., Пилиньский М., Рутковский Л. Нейронные сети, генетические алгоритмы и нечеткие системы / пер. с польск. И. Д. Рудинского. 2-е изд. М.: Горячая линия – Телеком, 2013. 384 с.
  21. Класифікація і характеристика експертних методів. URL: [https://pidruchniki.com/1677081363828/tovarovnavstvo/klasifikatsiya\\_harakteristika\\_ekspertnih\\_metodiv](https://pidruchniki.com/1677081363828/tovarovnavstvo/klasifikatsiya_harakteristika_ekspertnih_metodiv)
  22. Балашов П. А., Бакунина И. М., Кретов И. И. Оценка рисков информационной безопасности на основе нечеткой логики. *Безопасность компьютерных систем*. 2003. № 5. С. 56–59.
  23. Легчекова Е. В., Титов О. В. Метод расчета риска информационной безопасности. URL: <http://lib.ibteu.by/bitstream/handle/22092014/3600/Легчекова%20Е.В.%20Титов%20О.В.%20Метод%20расчета.pdf>
  24. Landoll D. *The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments*. New York : Boca Raton, 2006. 474 p. URL: [http://index-of.es/Misc/pdf/Auerbach.Publications.,The.Security.Risk.Assessment.Handbook.\(2005\).DDU.LotB.pdf](http://index-of.es/Misc/pdf/Auerbach.Publications.,The.Security.Risk.Assessment.Handbook.(2005).DDU.LotB.pdf)

## REFERENCES

- Alekseyev, A. "Upravleniye riskami. Metod CRAMM" [Management of Risks. CRAMM Method]. ЗАО «ИТ Эксперт». 2010. [https://www.itexpert.ru/rus/ITEMS/ITEMS\\_CRAMM.pdf](https://www.itexpert.ru/rus/ITEMS/ITEMS_CRAMM.pdf)
- Anikin, I. V. "Metod otsenki riskov dlya uyazvimostey informatsionnykh sistem, osnovanny na nechetkoy logike" [Risk Assessment Method for Information System Vulnerabilities Based on Fuzzy Logic]. *Informatsiya i bezopasnost*, vol. 17, no. 3 (2014): 468-471.
- Anikin, I. V., Yemaletdinova, L. Yu., and Kirpichnikov, A. P. "Metody otsenki i upravleniya riskami informatsionnoy bezopasnosti v korporativnykh informatsionnykh setyakh" [Methods for Assessing and Managing Information Security Risks in Corporate Information Networks]. *Vestnik tekhnologicheskogo universiteta*. 2015. <https://cyberleninka.ru/article/v/metody-otsenki-i-upravleniya-riskami-informatsionnoy-bezopasnosti-v-korporativnyh-informatsionnyh-setyah/viewer>
- Balashov, P. A., Bakunina, I. M., and Kretov, I. I. "Otsenka riskov informatsionnoy bezopasnosti na osnove nechetkoy logiki" [Information Security Risk Assessment Based on Fuzzy Logic]. *Bezopasnost kompyuternykh sistem*, no. 5 (2003): 56-59.
- Business Risk: websayt. <https://businessjargons.com/businessrisk.html?fbclid=IwAR0BhV81y0fe0V0JIEekCXgq0XjJK5ekWrycGn96R-zT-azxE7S82PeQVXY>
- Hozhyi, O., Kobylinskyi, I., and Luhinets, D. "Pidkhdid do otsiniuvannya ryzykiv u zadachakh planuvannia" [Approach to Risk Assessment in Planning Tasks]. *Visnyk Natsionalnoho universytetu «Lvivska politekhnika»*. Seriiia «Kompiuterni nauky ta informatsiini tekhnolohii». 2014. <http://ena.lp.edu.ua:8080/bitstream/ntb/25926/1/16-98-105.pdf>

- “Klasyfikatsiia i kharakterystyka ekspertnykh metodiv” [Classification and Characterization of Expert Methods]. [https://pidruchniki.com/1677081363828/tovaroznavstvo/klasifikatsiya\\_harakteristika\\_ekspertnih\\_metodiv](https://pidruchniki.com/1677081363828/tovaroznavstvo/klasifikatsiya_harakteristika_ekspertnih_metodiv)
- Korotnev, K. “Metodiki upravleniya riskami informatsionnoy bezopasnosti i ikh otsenki (chast 1)” [Information Security Risk Management Techniques and Their Assessment (Part 1)]. <https://safe-surf.ru/specialists/article/5193/587932/>
- Korotnev, K. “Metodiki upravleniya riskami informatsionnoy bezopasnosti i ikh otsenki (chast 2)” [Information Security Risk Management Techniques and Their Assessment (Part 2)]. <https://safe-surf.ru/specialists/article/5194/587935/>
- Krisevich, V. S. et al. *Ekspertnyye sistemy dlya personalnykh kompyuterov: metody, sredstva, realizatsii: sprav. posobiye* [Expert Systems for Personal Computers: Methods, Tools, Implementations: a Reference Guide]. Minsk: Vysh. shk., 1990.
- Landoll, D. “The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments”. [http://index-of.es/Misc/pdf/Auerbach.Publications,.The.Security.Risk.Assessment.Handbook.\(2005\).DDU.LotB.pdf](http://index-of.es/Misc/pdf/Auerbach.Publications,.The.Security.Risk.Assessment.Handbook.(2005).DDU.LotB.pdf)
- Legchekova, Ye. V., and Titov, O. V. “Metod rascheta riska informatsionnoy bezopasnosti” [Method for Calculating Information Security Risk]. <http://lib.ibteu.by/bitstream/handle/22092014/3600/Легчекова%20Е.В.%20Титов%20О.В.%20Метод%20расчета.pdf>
- Pastoyev, A. “Metodologii upravleniya IT-riskami” [IT Risk Management Methodologies]. Otkrytyye sistemy SUBD. 2006. <https://www.osp.ru/os/2006/08/3584582/>
- Pesotskaya, Ye. Yu. “Neobkhodimost upravleniya riskami v oblasti informatsionnykh tekhnologiy” [The Need for Risk Management in the Field of Information Technology]. *Sovremennyye problemy nauki i obrazovaniya*. 2007. <http://www.science-education.ru/ru/article/view?id=821>
- Rutkovskaya, D., Pilinskiy, M., and Rutkovskiy, L. *Neyronnyye seti, geneticheskiye algoritmy i nechetkiye sistemy* [Neural Networks, Genetic Algorithms and Fuzzy Systems]. Moscow: Goryachaya liniya – Telekom, 2013.
- Shorikov, A. F., and Butsenko, Ye. V. “Ekspertnaya sistema investitsionnogo proektirovaniya” [Expert System of Investment Design]. *Prikladnaya informatika*, no. 5 (2013): 96-103.
- Singina, A. A. “Vzglyad na upravleniye riskami informatsionnykh sistem” [A Look at Risk Management of Information Systems]. *Molodoy uchenyy*. 2011. <https://moluch.ru/archive/29/3284>
- Tkachenko, V. “Suchasni pidkhody do otsinky ryzykiv informatsiinykh tekhnolohii. Upravlinnia ryzykamy IT” [Modern Approaches to Information Technology Risk Assessment. IT Risk Management]. *Active Audit Agency*. 2010. <https://ppt-online.org/172211>
- “Upravleniye IT riskami” [IT Risk Management]. <https://www.itexpert.ru/rus/newsline/articles/detail.php?ID=8936>
- Vaskiv, O. M., and Shevchuk, Yu. I. “IT-ryzyky iak osnovne dzherelo biznes-ryzykiv” [IT Risks as the Main Source of Business Risks]. *Polish Journal of Science*, no. 20 (2019): 28-36.
- Vaskiv, O. M., and Shevchuk, Yu. I. “IT-ryzyky ta yikh zviazok z biznes-ryzykamy” [IT Risks and Their Relation to Business Risks]. *The Modern Economic Research: Theory, Methodology, Practice: Conference Proceedings*. Kielce, Poland: Baltija Publishing, 2019. 78-82.
- Voronko, R. M. “Otsinka ta kontrol biznes-ryzykiv subiektyv hospodariuvannia spozhyvchoi kooperatsii Ukrainy” [Evaluation and Monitoring Business Risk of Business Entities of the Consumer Cooperation of Ukraine]. *Visnyk Natsionalnoho universytetu «Lvivska politekhnika»*. Seriya «Menedzhment ta pidpriemnytstvo v Ukraini: etapy stanovlennia i problemy rozvytku». 2017. [http://ena.lp.edu.ua:8080/bitstream/ntb/41599/2/2017n862\\_Voronko\\_R\\_M-Evaluation\\_and\\_monitoring\\_40-48.pdf](http://ena.lp.edu.ua:8080/bitstream/ntb/41599/2/2017n862_Voronko_R_M-Evaluation_and_monitoring_40-48.pdf)
- “What board members need to know - and do. Information technology risks in financial services”. <https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-ccg-information-technology-risk-in-fs.pdf>
- Yesieieva, I. V., and Moskalenko, V. O. “Osnovni vydy ryzykiv ta yikh vplyv na konkurentospromozhnist molokoperobnykh pidpriemstv” [The Main Types of Risks and Their Impact on the Competitiveness of Dairy Enterprises]. *Ekonomika i orhanizatsiia upravlinnia*. 2014. <http://jeou.donnu.edu.ua/article/view/1092/1110>