ORIGINAL PAPER

DOI: 10.26794/2308-944X-2021-9-3-94-102
JEL C13, C53, D21, D81, J31

About Some Risks Associated with Subjective Factors, and the Methodology for their Assessment

Aleksandr Kozlov[a], Nikolai Noga[b]

[a]Complex Networks Lab, Trapeznikov Institute of Control Sciences, Russian Academy of Sciences, Moscow, Russia
https://orcid.org/0000-0001-8615-0883,
[b]Complex Networks Lab,
Trapeznikov Institute of Control Sciences, Russian Academy of Sciences, Moscow, Russia
https://orcid.org/0000-0003-4929-8736,

ABSTRACT

The authors propose a methodology for assessing the risk associated with subjective factors that may affect the achievement of the final goals of business projects, including ensuring information security. Such factors may include the level of salary, the level of professionalism, and others. At the same time, we propose carrying out the risk assessment by using the fuzzy logic method, which allows us to determine the dependence of the risk on various parameters under conditions of their uncertainty. According to the authors, the proposed methodology will help avoid some incorrect management decisions in the formation of author (working) teams, which could lead to negative consequences in the further implementation of the business project. These negative consequences can be expressed in delaying the implementation period, increasing the project's cost, or even losing business due to critical information and personnel leakage. Also, this method allows you to increase the effectiveness of personnel policy in the organisation or the company. We noted that this method is applicable not only for individual enterprises but also for corporations and associations with complex network structures.

Keywords: business project; qualified leak; information security; external and internal violator; human factor; fuzzy logic; risk management

For Citation: **Kozlov, A., & Noga, N. (2021). About some risks associated with subjective factors, and the methodology for their assessment. *Review of Business and Economics Studies, 9*(3),94-102. doi:10.26794/2308-944X-2021-9-3-94-102**

ОРИГИНАЛЬНАЯ СТАТЬЯ

О некоторых рисках, связанных с субъективными факторами, и методика их оценки

Александр Козлов[a], Николай Нога[b]

[a]Институт проблем управления, Российская академия наук, Москва, Россия
[b]Институт проблем управления, Российская академия наук, Москва, Россия

АННОТАЦИЯ

Авторами предложена методика оценки риска, связанного с субъективными факторами, которые могут оказывать влияние на достижение конечных целей бизнес-проектов, включая обеспечение информационной безопасности. В качестве таких факторов могут выступать: уровень зарплаты, уро-

вень профессионализма и другие. При этом оценку риска мы предлагаем проводить с помощью метода нечеткой логики, что позволяет определять зависимость риска от различных параметров в условиях их неопределенности. По мнению авторов, предлагаемая методика поможет избежать некоторых неправильных управленческих решений при формировании авторских (рабочих) коллективов, которые могли бы привести к негативным последствиям при дальнейшей реализации бизнес-проекта. Эти негативные последствия могут выражаться в затягивании сроков реализации, удорожании самого проекта или даже потере бизнеса из-за утечки критически важной информации и кадров. Представленная авторами методика позволяет повысить эффективность проведения кадровой политики не только в отдельных организациях, но и в корпорациях и объединениях, имеющих сложные сетевые структуры.
***Ключевые слова*:** бизнес-проект; квалифицированная утечка; информационная безопасность; внешний и внутренний нарушитель; человеческий фактор; нечеткая логика; управление риском

1 Introduction

In current conditions, any organisation (enterprise) starting a new business project must determine the purpose (aim) of this project, the necessary funds and resources for its implementation, and possible risks.

The document titled GOST R ISO 31000–2019 "Risk Management. Principles and guidelines" defines risk as: "the consequence of the influence of uncertainty on the achievement of aims".

This influence can lead to a deviation in achieving the aim. The deviation can be expressed as a failure of deadlines, an increase in costs, or even a complete failure of the project and, as a result — the loss of business.

The longer the project's duration, the more likely it is that its implementation's external and internal conditions will change. It means that long-term projects are a priori riskier than short-term ones.

Currently, no solid business project is complete without the use of information technology. And these technologies both help to speed up all processes and bring with them new threats and risks.

According to the InfoWatch group of companies, for the first nine months of 2020, 7.4 per cent fewer leaks were registered in the world than in the same period last year [InfoWatch, 2020]. On the contrary, in Russia, the number of leaks increased by 5.6 per cent over the same period. From January till September 2020, 9.93 billion records of personal data and payment information were leaked worldwide, of which 96.5 million were in Russia. The leaks distribution by data type we present in Table 1.

During the same period, 52.6 per cent of leaks worldwide occurred due to external influences. At the same time, there was only 21 per cent of such leaks in Russia, and more than 79 per cent of leaks occurred due to internal violations. If a little more than half of the violations of an internal nature are recognised as intentional in the world, then in Russia, there are more than 3/4 of such violations. In Russia, the share of leaks caused by employees is twice as high as in the world — more than 72 per cent. The leaks distribution by culprit we present in Table 2.

More than 40 per cent of registered leaks in Russia are in the high-tech and financial sectors — 21.9 per cent and 18.9 per cent of cases, respectively. In the world, the high — tech sector is in the first place with a share of 19.4 per cent, and healthcare is in second place — 16.4 per cent.

In Russia, the share of leaks associated with fraudulent activities is three times higher, 10.3 per cent versus 3.3 per cent. It means that violators, primarily internal ones, still have many loopholes to take advantage of information stolen from the corporate circuit for direct profit.

The main channel of leaks remains the Network (Browsers and the Cloud).

Also, in Russia, the share of leaks through paper documentation remains relatively high. Despite the rapid development of electronic document management in recent years, a significant part of the data is still stored and transmitted on paper.

The statistic shows that in 2019 internal leaks of information constituting a trade (commercial) secret occupy firmly the second place after the undisputed leader — internal leaks of personal data: 75 and 12 per cent, respectively.

At the same time, it should be borne in mind that leaks of information constituting a commercial secret are intentional in 80 per cent of cases. Leaks of personal data, on the contrary, are mostly accidental.

In the case of user data, more than half of the leaks are accidental. In the case of other types of data, most of the leaks occur due to deliberate actions. Intentional leaks count for commercial secrets

Table 1
Distribution of leaks by data type: Russia-World, January-September 2020

Type of the data	In Russia (%)	In the world (%)
Personal information	85.9	80.1
Payment (financial) information	2.0	5.6
State secret	6.7	4.7
Business secrets, know — how	5.4	9.6

Source: The authors.

(80 per cent), production secrets (88 per cent), and state secrets (85 per cent).

At the same time, internal intentional leaks have high latency. An internal violator "targeting" the theft of the employer's trade secrets is usually well aware of where the information of interest is stored, how and who controls the data transmission channels. As a result, the leak of commercial secrets is either not recorded at all or is discovered by the affected company after the fact.

Internal leaks have powerful destructive potential. The consequences of mistakes or malicious actions of personnel can manifest themselves in property or reputational losses and the suspension or liquidation of the business.

The factors influencing the actions of the internal violator are usually subjective and have a corruption component at their core [Kozlov & Noga, 2019]. When assessing the risk of implementing a business project, it is necessary to consider these factors.

2 Subjective Risk Factors

What motivates the internal violator? The main reasons are greed and negligence. The self-serving and psychological motives for violations are almost the same as those of corruption [Vannovskaya, 2013]:

- The employee's opinion that his work is undeservedly undervalued
- A significant difference in different categories of employee's wage
- High staff turnover, the presence of "temporary workers", including among managers
- Lack of individual employee interest in achieving the project aim, personal dissatisfaction
- Low qualification of the employee, his inability to work on equal terms
- Company tolerance to minor violations
- The presence of double standards in the organisation when a certain category of employees (managers) is allowed to violate the established rules. The employee believes that this is cheating him, and he also has the right to cheat
- Excessive bureaucracy and insufficient control, when it is easier to circumvent the rules than to comply with them.

Risk Parameters

Consider the above factors as some parameters that affect the value of risk in the organisation. The level of material satisfaction consists of wage and household comfort. Several parameters can define this level:

- The value of the deviation of the average wage in the team from the average salary in the industry (region)
- The ratio of the average wage in the team to the average wage in the industry
- The spread of employees' wages (how much they differ in the team), its dispersion.

The authors propose representing wage dispersion as the standard deviation from the average value, well described by the variance of a discrete random variable — wage:

$$D(z) = M(z - M(z))^2, \quad (1)$$

where D (z) is the wage dispersion (the average of the square of the deviation of the wage from the average level), z — is a random variable — the employee's wage, M (z) — is the average wage in the team.

According to the author's opinion, another important parameter that affects the organisation's risk is the professional level of employees. This level can be represented as the ratio of the average employees work experience in this area (in this direction) to the average life cycle of products (products) produced by this company.

Under the product life cycle, we will understand the time required for its development, testing, organisation of production, production cycle, the period

Table 2
Distribution of leaks by violators: Russia — World, January — September 2020

Leak's violator	In Russia (%)	In the world (%)
Head manager	5.0	2.6
System Administrators	0.0	0.1
Unprivileged employees	72.1	36.5
Former employees	2.0	0.9
Contractors	1.0	2.2
External attackers	29.1	57.7

Source: The authors.

of implementation and operation, during which its technical support is carried out.

Thus, the professional level can be represented in the following form:

$$P = \frac{\sum_{i=1}^{n} S_i}{nG}, \quad (2)$$

where P — is the level of professionalism, S_i — is the employee's work experience in this field, n is the number of employees in the team, and G — is the average life cycle of the products produced.

At the same time, it is worth noting that the more technologically complex products usually have longer life cycles. So, for example, it can take ten or more years to develop an entirely new computer processor based on new architectural principles or create a new aircraft. And to launch it into production with the solution of numerous organisational issues may take as many more years.

Also, the following parameters can be attributed to subjective risk factors:

• The level of the employee's interest in the results of the work, defined as the time of work on this project (usually, if the employee is interested in the result, then he tries, all other things being equal, to stay in the team until the final result is obtained)

• The level of comfort in the team can be determined by the parameter — the lifetime of the stable core of the team (the stable core of the team). If it were not comfortable to work in this team, then employees would try to leave it, and there would be a significant turnover of personnel

• The level of commitment to the company's goals is a parameter similar to the previous one, only, in this case, it refers to a large company and is instead an individual parameter for a particular employee, i.e., the longer the employee's work experience in this company, the higher the level of commitment

• The level of compliance of the vector of decisions made with the company's goals and their impact on other team members. This parameter rather refers to top managers who make decisions or influence the adoption of certain managerial decisions. For example, a company produces aeroplanes or cars but has faced some financial issues. The financial manager, first of all, should reduce expenses. But, if at the same time to reduce the division of designers — designers, so in the future will not be created new aircraft or cars and the company will not be competitive, and may even lose business.

The human (subjective) factor is essential when assessing the risk for any enterprise and high-tech companies working with new technologies — especially. Underestimating this can negatively affect the performance of the enterprise (company).

Therefore, it is necessary to maintain a decent wage level, strive to maintain and, if possible, create a healthy climate in the team based on the professionalism of its employees and provide opportunities for career and material growth to reduce the risk associated with subjective factors.

But how to assess this risk depend on the listed parameters, which is not clearly expressed?

In this case, the authors suggest using the fuzzy logic method for its evaluation and using the MATLAB Fuzzy Logic Toolbox package for its implementation [Matlab, 2019].

3 Risk Assessment

In assessing the risk according to the proposed methodology, it is possible to build the depend-

Table 3
Wage (salary) level

N	Wage level	Possible actions of employees	Relation to the average wage in the sector	The boundaries of the term "Wage level"
1	Low	Employees ' desire to find another job or to sell secrets	0.1–0.75	0.1–0.4
2	Middle	Stable job, but getting a better offer, leave your job	0.75–1.50	0.4–0.6
3	**High**	**The desire to maintain this level**	**More 1.50**	**0.6–1.0**

Source: The authors.

Table 4
Wage dispersion level

N	Wage dispersion level	Possible actions of employees	The boundaries of the term "Wage dispersion level"
1	High	Employees' desire to find another job or to sell secrets	0.7–1.0
2	Middle	Stable job, but getting a better offer, leave your job	0.3–0.8
3	**Low**	**The desire to maintain this level**	**0.1–0.4**

Source: The authors.

ence of the risk on all of the above parameters and some other specific ones to specific enterprises. But in this case, the description and calculation will be pretty time-consuming. A variant of the risk assessment with dependence on five parameters is given in the paper [Kozlov & Noga, 2020].

For simplicity and clarity, we will evaluate the dependence of risk on three parameters, which, according to the authors, are one of the main parameters that influence subjective risk factors.

In the proposed example, these parameters will be:

- The wage level *U(z)* — the ratio of the average salary in the team *M (z)* to the average wage in the industry *M*
- The wage dispersion level in the team *D(z)*
- The professional level of the employees *P*.

In this case, the risk R can be represented as a function of these parameters.

$$R = R(U(z), D(z), P) \quad (3)$$

The fuzzy logic method involves working with linguistic variables. The correspondence of linguistic variables to the above parameters we show in Tables 3–5. We will consider all variables normalised with values in the range from 0 to 1.

If the company's wage level is significantly lower than the average in the industry, then the company will inevitably face problems with recruiting qualified specialists. The exception may be cases of temporary difficulties with the prospect of overcoming them in the future.

Significant dispersion of the employees' wage in the team can also cause many negative cases, such as envy and betrayal of the company's interests based on "underestimating" the personal employee's contribution.

Moral and material dissatisfaction can push an employee (employees) to find a new job with better working conditions and simply to sell the technical and technological secrets of the company.

The professional level also has a significant impact on the risk assessment. The lower this level, the more likely it is to make mistakes that can lead to the failure of the project deadlines, its price rise, or even to the inability to achieve the aim.

In addition, less professional employees are more prone to overestimating their importance and sometimes do not listen to the opinions of more experi-

Table 5
Professional level

N	Professional level	Possible consequences	The boundaries of the term "Professional level"
1	Low	Possible adoption of technically incorrect decisions	0.1–0.3
2	Middle	Increasing the project implementation time, reducing its quality due to insufficient experience	0.3–0.8
3	High	There may be minor deviations in the implementation time	More 0.8

Source: The authors.

Table 6
Output variable Risk (yR)

	Risk level	The boundaries of the term "Risk level"
1	Insignificant	0.0–0.20
2	Acceptable	0.16–0.50
3	High	0.45–1.00

Source: The authors.

enced employees. And if they are also top managers, head of the team or company divisions with the vote right, then the consequences can be very harmful. The linguistic variable with the corresponding professional level we show in Table 5.

Finally, an approximate risk estimation algorithm based on the provisions of fuzzy logic and fuzzy set theory, considering the uncertainties that arise in any organisation, can be implemented using the as mentioned above MATLAB Fuzzy Logic Toolbox package. When using the production rules of fuzzy logic, we reproduce the output mechanism taking into account the three input variables. Such variables for assessing the risk associated with subjective (human) factors in our example, as already mentioned above, are:

- wage level
- wage dispersion level
- employees professional level.

Each of the listed input variables, as indicated above, is evaluated on its own scale. Next, these input variables are passed to the Fuzzy Logic Toolbox, and the output is the value of the output variable — risk.

As a visual example, consider a simplified risk calculation in the Fuzzy Logic Toolbox with three input variables: wage level — $x_{Z,}$ wage dispersion level — x_D, and professional level — $x_{P.}$

There is the variable risk — y_R (Risk). That is, now equation (3) has the following form

$$y_R = R\,(x_Z, x_D, x_P). \quad (4)$$

We apply the Mamdani model and assume that the membership functions of the three variables have a trapezoidal form. The risk membership function has the shape of a Gaussian curve. The ranges of changes in terms specified in Tables 3–5, respectively, are used to evaluate the input variables. For the output variable y_R, we use three terms with the measurement range specified in Table 6.

Further, to form a fuzzy knowledge base, we introduce production rules, partially presented in Table 7.

A graphical representation of the Mamdani knowledge base in the Fuzzy Logic Toolbox rules editor we show in Figure 1.

After defuzzification, you can get a specific value of the output risk parameter for specific values of the input variables and compare it with the acceptable value. The presented package allows you to visualise the dependence of the risk on the input parameters (4).

According to the given input parameters, it is possible to build three three-dimensional graphs. At the same time, on each of them, you can see the dependence of the risk for two parameters with fixed values of the third. To determine the optimal values of the parameters with an acceptable

Table 7
Fuzzy knowledge base, production rules

N	Wage level	Wage dispersion level	Professional level	Risk level
1	Low	High	Low	High
2	Low	High	Middle	High
3	Low	High	High	High
4	Low	Middle	Low	High
…	…	…	…	…
24	High	Middle	High	Insignificant
25	High	Low	Low	Acceptable
26	High	Low	Middle	Insignificant
27	High	Low	High	Insignificant

Source: The authors.

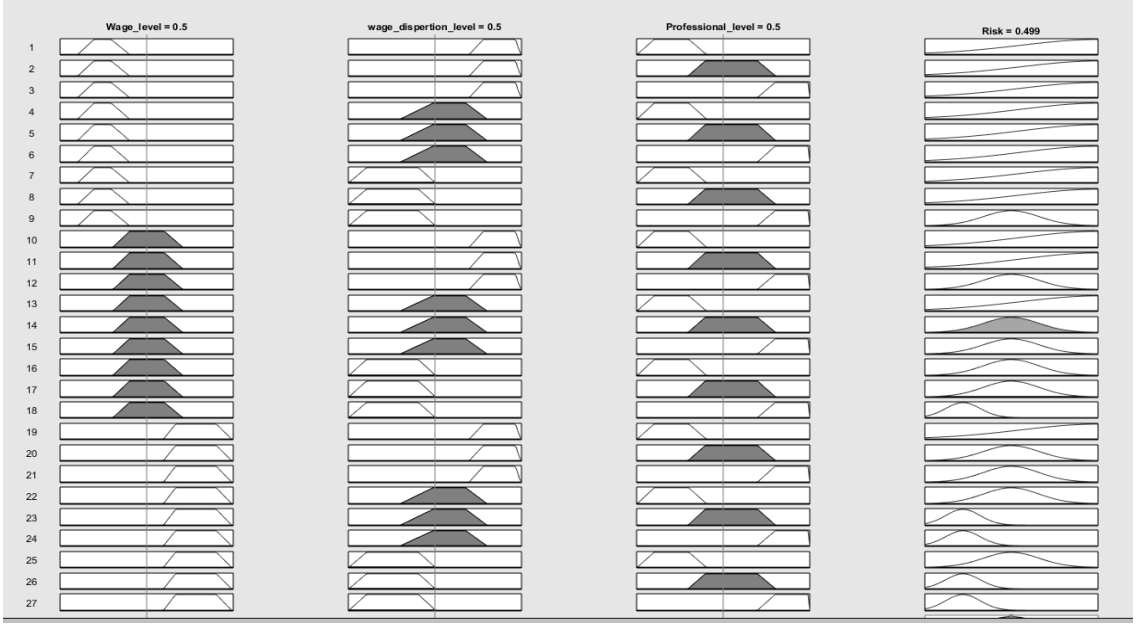

Figure 1. Mamdani's fuzzy knowledge base in the Rules Editor.

Source: The authors.

risk value, you need to do some work, varying the values of the input parameters. Naturally, this is only possible within the limits of the restrictions imposed on these values, which are available to implement real projects.

Figure 2 shows a visualisation of the risk dependence at the wage dispersion level and the wage level. This relationship indicates that the smaller the wage dispersion level in the team and the higher the overall wage level, the lower risks associated with the manifestation of subjective (human) factors.

You can also visualise the risk dependence at the professional level and the wage level (Figure 3), the professional level and the wage dispersion level (Figure 4). In this example, to simplify the presentation of the basic principles of the proposed method for assessing the dependence of risk on subjective factors, each linguistic variable corresponds to only three intervals of values. In fact, you may need more of them to get more accurate results. And there may be more variables themselves. For example, to assess the level of wage, it may be necessary to compare it with the level of living in a given country and the wage level of a specialist in a given professional field in other countries.

It is necessary to understand that the further use of new values and new variables increases the number of production rules and complicates their writing. It, in turn, may lead to the need to attract additional experts.

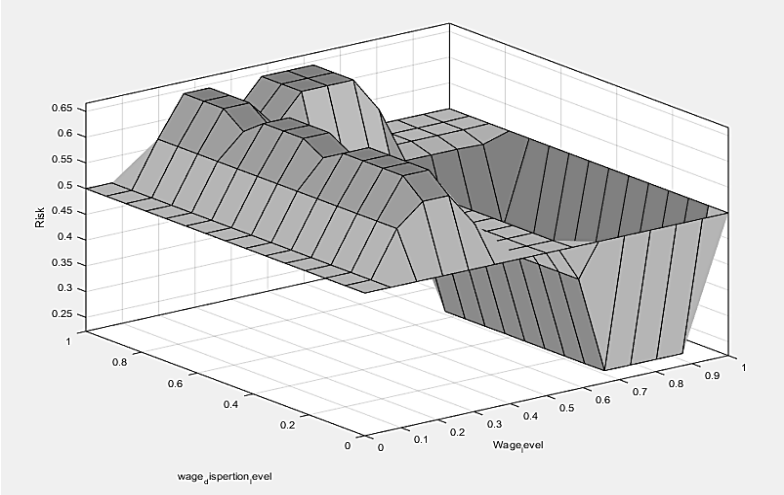

Figure 2. Visualisation of the risk dependence at the wage dispersion level (x_D) and the wage level (x_Z)

Source: The authors.

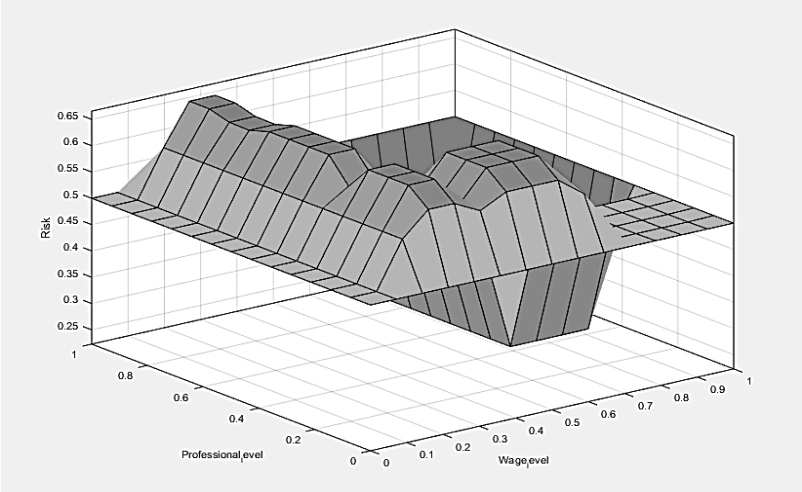

Figure 3. Visualisation of the risk dependence at the professional level (x_P) and the wage level (x_Z).

Source: The authors.

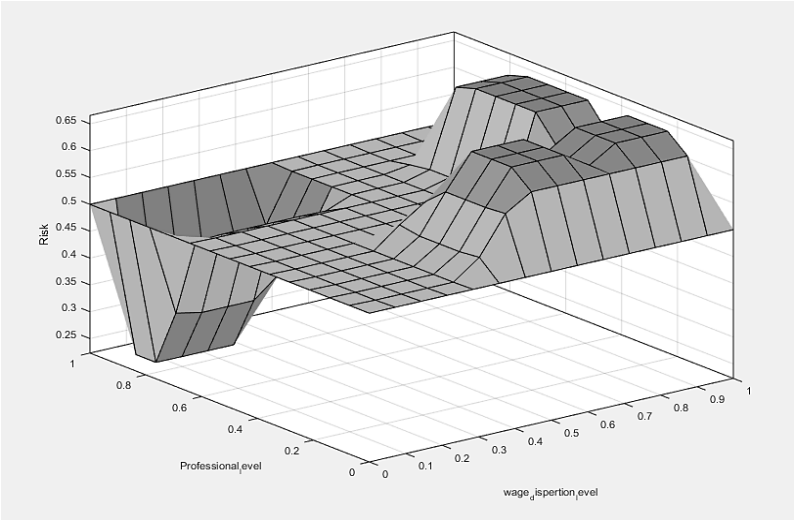

Figure 4. Visualisation of the risk dependence at the professional level (x_P) and the wage dispersion level (x_D).

Source: The authors.

4 Conclusion

The proposed method allows us to assess the dependence of risk on subjective factors that are difficult to describe mathematically strictly. The article provides an example of evaluating the dependence of risk at the wage level, the wage dispersion (spread) level and the professional employees level. This method allows us to assess the dependence of risk on other subjective parameters, both those given in this paper and those that may be specific only for specific enterprises or company.

Using the above methodology, in conditions of great uncertainty and non-obvious mutual influence of parameters at different stages of the life cycle of various business projects, it becomes possible:

1. Determine the impact of various subjective risk factors on the level of a particular business project implementing risk

2. Assess the level of risk, both at the moment and at various stages of the business project life cycle

3. Optimise the personnel policy of the enterprise (organisation), which reduces the risk of leakage of high-tech (know-how) information, as well as the leakage of "brains", to stabilise the staff

4. Develop recommendations for the formation of a healthy atmosphere in the team, which will allow you to optimally solve the tasks set to achieve the aims of the business projects

5. Avoid erroneous management decisions, especially those related to the company or staff "optimisation".

The proposed methodology can be used in individual enterprise and organisations with a complex network structure. For example, there may be a company with a large number of branches. If so, it is necessary to compare the wage level not within the team but between branches.

References

InfoWatch. (2020). Restricted Information leaks: report for 9 months of 2020. Retrieved from: https://www.infowatch.ru/form — modal/report — download/30708. (Accessed 08.03.2021).

InfoWatch, (2020), Data leaks of organisations due to the fault of an internal violator. Comparative study. 2013–2019. Retrieved from: https://www.infowatch.ru/form — modal/report — download/24339. (Accessed 08.03.2021).

Kozlov A., Noga N. (2020). Some Method of Complex Structures Information Security Risk Assessment in Conditions of Uncertainty. Proceedings of the 13th International Conference "Management of Large-Scale System Development" (MLSD). Moscow: IEEE. Available at: https://ieeexplore.ieee.org/document/9247662.

Kozlov A., Noga N. (2019), The Information Security Risks of Enterprise Information Systems Using Cloud Technology, *Risk management*, *3*, 31–46. (In Russian).

Matlab version 9.6.0 R 2019a [Electronic resource]. Available at: https://1progs.ru/matlab/. (Accessed 05.09.2019).

Vannovskaya O.V. (2013). *Psychology of corrupt behaviour of civil servants*. St. Petersburg: Ltd "Book House"; 264 p. (In Russian)

ABOUT THE AUTHORS / ИНФОРМАЦИЯ ОБ АВТОРАХ

Aleksandr Kozlov — Research Officer Complex Networks Lab, Trapeznikov Institute of Control Sciences, Russian Academy of Sciences, Moscow, Russia
alkozlov@ipu.ru
Александр Козлов — научный сотрудник лаборатории «Сложные сети» института проблем управления, Российская академия наук, Москва, Россия

Nikolai Noga — Research Officer Complex Networks Lab, Trapeznikov Institute of Control Sciences, Russian Academy of Sciences, Moscow, Russia
noga@ipu.ru
Николай Нога — научный сотрудник лаборатории «Сложные сети» института проблем управления, Российская академия наук, Москва, Россия

The article was submitted on 17.05.2021, reviewed on 16.07.2021, and accepted for publication on 17.08.2021.
The authors read and approved the final version of the manuscript.
Статья поступила в редакцию 17.05.2021; после рецензирования 16.07.2021; принята к публикации 17.08.2021.
Авторы прочитали и одобрили окончательный вариант рукописи.