Researching of firewall capabilities during organizing multi-user work

L V Stepanov¹, R V Kuzmenko¹, R S Mokshin¹, D B Desyatov¹ and D G Zybin¹

¹Voronezh institute of the Russian Federal Penitentiary Service, Russia, Voronezh, Irkutskaya 1a

E-mail: stepanovlv@yandex.ru

Abstract. Fundamental concept in human life is a concept of a «system». This concept is extended to all of the directions of the human’s activity. A great number of the economic, engineering, biological and many others kinds of the objects are rather complicatedly organized systems. Any system has a great number of parameters which characterize its organization and operation. Among these parameters a special point is associated with system safety. It can be determined as a state of system immunity to the different destructive impacts which can have a negative effect on its operation and/or its structure. In any variant of consideration this system is formed by participants of some relationships and it can have as organizational, as technical or some other nature at one and the same time. Examples of the organizational systems are enterprises, offices and organizations. Examples of the technical structures are infocommunication, telecommunication systems and networks. The performed analysis means a system character not only of the system safety, but also indicates at the aspects that determine safety. Moreover, it is possible to reveal a conflict character of interaction between some aspects of the system safety. This occasion provides a reasonable application for the simulation of the systems in the game theory. Examples of this application are also presented in this article.

1. Introduction

One can quite clearly state that the property of safety itself is of systemic character [1, 2]. In a majority of cases system safety is determined by:

1) threats – are capable in reality or in potential to influence the system;
2) vulnerabilities – which can have:
   - subjective character – they appear due to insufficient engineering, organizational or economical solutions realized in the office;
   - objective character – they can appear as a result of the absence or insufficient efficiency of the engineering, organizational or economical measures at the modern stage of development;
3) measures providing the safety – a complicated activity directed either at the countermeasures to the threats or at the elimination of the system vulnerabilities.

For example, failure to perform Federal normative documents in the systems concerning content of the confidential information can result in the formation of vulnerabilities of the organizational character. The use of inefficient means of struggle with a scumware in the telecommunication systems can develop vulnerabilities of the technical kind.
Figure 1. Aspects of system safety.

Regardless of the type of the considered system there is always a possibility of the presence of a party desiring to decrease the safety level. It means that there is an intruder and an opposite party realizing the measures on the prohibiting of this phenomenon.

Nevertheless, a situation is possible when the measures concerning safety provision can be directed not at the counteraction to the threats themselves but at the elimination of the vulnerabilities in the system and vice versa.

Threats, vulnerabilities and measures concerning provision of the safety have a compound structure. They can have a number of characteristics and each of them is presented by several parameters. For example, a threat to the confidentiality of information can become apparent in disclosure, leakage and/or unauthorized access to the information. In this example disclosure of the information is determined by the following parameters: format of the message, reliability of the content or transmission, probability of loss and some others.

Figure 2. Interrelation of the aspects providing system safety.

Hence, in order to estimate protection of the system it is required to correlate threats, vulnerabilities and measures on the safety provision between each other.

2. Statement and analysis of the problem from the viewpoint of game theory
With the account of the chosen approach we can state the problem. Assume that an intruder disposes four means of software, engineering or program-technical kind which can have a negative effect on the
safety of the office. Suppose that threats have the following factors: cost, index of the destructive action and certain labor intensiveness of application for the intruder. While performing observation of the safety in the office there were found vulnerabilities of the system in the amount of three cases. Elimination of these vulnerabilities by the employees requires a set of the measures which are characterized by: their value, efficiency of the measures and cost-based value of the measures for an office. Let us make an assumption that elimination of one vulnerability is possible by the realization of not a single measure. And vice versa, intruder can realize several threats. Thus, it is required to assess the level of a system safety for an office.

3. **Group-theoretical approach to the assessment of the system safety**

As it follows from the statement of the problem, one of the indices – the cost of threats and vulnerabilities are described by the quantitative values while all the other parameters are described as qualitative ones. The latter ones can be assessed by the linguistic constructions of the type: high, middle, low. It means the use of different scales [3, 4].

There are different approaches in the processing of fuzzy data. At present, there are certain methods based on the latent variables [5, 6], as well as a theory of fuzzy sets. These mathematical approaches possess certain advantages and drawbacks. One of the drawbacks is a complexity of the practical use in the models that would be accessible for application by the employees of the real offices and departments.

A transition from the linguistic constructions to their numerical expression can be done with the use of the expert assessment or basing on the matrix of pairwise comparison for these constructions. As a result, the relative values will be obtained. In order to get the common energy scale the cost indices should be normalized. As a result, matrices of the uniform values will be obtained.

While calculating an integrated estimate for each of the threats and vulnerabilities it should be taken into account that certain parameters can make positive contribution, but some of them – the negative one. For example, disruptiveness of a threaten is a positive value from the viewpoint of intruder while programming labor is a negative one. At the same time, for the measures efficiency has a positive value, while programming cost is negative one. Considering all of these moments corresponding aggregate values will be calculated.

**Table 1.** Characteristics of the threats to the system safety.

| Value | Disruptiveness | Programming labor |
|-------|----------------|-------------------|
| Threat 1 | 0.35 | 0.58 | 0.35 |
| Threat 2 | 0.47 | 0.12 | 0.07 |
| Threat 3 | 0.18 | 0.3 | 0.58 |

**Table 2.** Integrated estimate of threats to the system safety.

| Integrated estimate |
|---------------------|
| Threat 1           | -0.12 |
| Threat 2           | -0.42 |
| Threat 3           | -0.46 |

**Table 3.** Characteristics of vulnerabilities for the system safety.

| Cost     | Efficiency | Costs |
|----------|------------|-------|
| Vulnerability (Measure) 1 | 0.26 | 0.35 | 0.58 |
| Vulnerability (Measure) 2 | 0.11 | 0.07 | 0.07 |
| Vulnerability (Measure) 3 | 0.63 | 0.58 | 0.35 |
Table 4. Integrated estimate of vulnerabilities in the system safety.

|                     | Integrated estimate |
|---------------------|---------------------|
| Vulnerability (Measure) 1 | -0.49               |
| Vulnerability (Measure) 2 | -0.11               |
| Vulnerability (Measure) 3 | -0.4                |

It should be noted that the negative values of the integrated estimate are connected with the fact that only one characteristics made a positive contribution into the estimate. In the real conditions for a great number of parameters positive values can be obtained along with the negative ones. One can also take into account that a certain characteristic may be of defining value for the estimate of a threat or vulnerability. To account for this fact the additional weight coefficients can be introduced.

Keeping in mind core items of the games theory the detected threats and vulnerabilities of an office represent in fact strategies of an intruder and strategies of an office concerning vulnerabilities elimination. Hence, the integrated estimates of the strategies provide a possibility to pass to the formation of matrix of the game interaction between the participants of the considered system. It should be also specially noted that this interaction is obviously of a confrontation kind, i.e. it is antagonistic one. This is reason that substantiates application of matrix games theory for the simulation of interaction between intruder and office [7].

Table 5. Game matrix.

|                  | Player 1 | Player 2 |
|------------------|----------|----------|
|                  | 1        | 2        | … | m |
| 1                | x_{11}   | x_{12}   | … | x_{1m} |
| 2                | x_{21}   | x_{22}   | … | x_{2m} |
| …                | …        | …        | … | … |
| n                | x_{n1}   | x_{n2}   | … | x_{nm} |

In this variant of the problem statement different ways for calculations of the values for matrix elements are possible. Keeping in mind that the article pursues the aim of the study – a possibility of application of the games theory to the assessment of the system safety we shall determine the values of matrix elements as the difference between the values of vulnerabilities parameters (measures) and the estimates of threats. As a result, game matrix can be obtained.

Table 6. Game matrix for «Intruder-office» game.

|                     | Threat | -0.49 | -0.11 | -0.4 |
|---------------------|--------|-------|-------|-------|
| -0.12               | -0.37  | 0.01  | -0.28 |
| -0.42               | -0.07  | 0.31  | 0.02  |
| -0.46               | -0.03  | 0.35  | 0.06  |

After formation of the matrix it is required to check a possibility of searching the game solution in pure strategies:
\[
\min \max (a_{ij}) = \max \min (a_{ij})
\]  

(1)

**Table 7.** Solution of the matrix game in pure strategies.

| Threat | Vulnerability (Measure) | Min | Max |
|--------|-------------------------|-----|-----|
| -0.49  | -0.11                   | -0.4| -0.37|
| -0.12  | 0.01                    | -0.28| -0.07|
| -0.42  | 0.31                    | 0.02 | -0.03|
| -0.46  | 0.35                    | 0.06 | -0.03|
| -0.03  | 0.35                    | 0.06 | -0.03|

Application of minimax and maximin approach to the represented game matrix allows determining that a saddle point surely exists here.

The obtained result needs to be interpreted. To do this it is required to compare the data in Tables 1-4 with the results in Table 7. For the intruder most reasonable is the application of a third strategy, while for the office it is the realization of the first strategy. In the considered problem the threats and complexes of measures correspond to these strategies, respectively. According to the provisions of the matrix game theory deviations from these strategies do not appear to be sufficiently reasonable since it may lead to deterioration of the result. If intruder deviates from this strategy then programming labor for the application of a scumware increases or reduces its disruptiveness, while the costs for the office also increase or efficiency of the measures decreases as compared with the threats of intruder. This conclusion is confirmed by the numerical data in the Tables 1 and 3. Solution of the game is of the negative value. It means that the measures concerning elimination of the vulnerabilities prove to be quite insufficient in regard to the actions of intruder. However, the value of deviation is quite insignificant and is close to zero.

If solution in the pure strategies is absent, then it should be searched in the mixed strategies. The search can be realized basing on the different methods; one of these methods is a linear programming technique.

**Figure 3.** Example of the game matrix for the case of mixed strategies.

Application of the linear programming allows obtaining:
x₁ + x₂ + x₃ + x₄ \rightarrow \text{min}  
\begin{align*} 
0.09x₁ + 0.51x₂ + 0.25x₃ + 0.51x₄ & \geq 1; \\
-0.33x₁ + 0.10x₂ - 0.17x₃ + 0.10x₄ & \geq 1; \\
-0.34x₁ + 0.08x₂ + 0.09x₃ + 0.08x₄ & \geq 1; \\
0.09x₁ + 0.51x₂ + 0.25x₃ + 0.51x₄ & \geq 1; 
\end{align*}  
\tag{2}

x₁ \geq 0; \ x₂ \geq 0; \ x₃ \geq 0; \ x₄ \geq 0.

y₁ + y₂ + y₃ + y₄ \rightarrow \text{max}  
\begin{align*} 
0.09y₁ - 0.33y₂ - 0.34y₃ + 0.09y₄ & \leq 1; \\
0.51y₁ + 0.10y₂ + 0.08y₃ + 0.51y₄ & \leq 1; \\
0.25y₁ - 0.17y₂ + 0.09y₃ + 0.25y₄ & \leq 1; \\
0.51y₁ + 0.10y₂ + 0.08y₃ + 0.51y₄ & \leq 1; 
\end{align*}  
\tag{3}

y₁ \geq 0; \ y₂ \geq 0; \ y₃ \geq 0; \ y₄ \geq 0.

In order to find solutions we use software add-on «Search for solution» in Excel.

| Vulnerabilities/Measures | Threats |
|-------------------------|---------|
| x₁  x₂  x₃  x₄  | F(x)   | y₁  y₂  y₃  y₄  | F(y)   |
| 0   0.2346 0.6562 11.413 | 12.3   | 0 0.4129 11.891 0 | 12.3   |
| 0.09 0.51 0.25 0.51 | 6.0811 | 0.09 -0.33 -0.34 0.09 -4.196 |
| -0.33 0.10 -0.17 0.10 | 1      | 0.51 0.10 0.08 0.51 1 |
| -0.34 0.08 0.09 0.08 | 1      | 0.25 -0.17 0.09 0.25 1 |
| 0.09 0.51 0.25 0.51 | 6.0811 | 0.51 0.10 0.08 0.51 1 |
| V  p₁  p₂  p₃  p₄  | V  p₁  p₂  p₃  p₄  | 0.081 0 0.019 0.053 0.928 0.081 0 0.034 0.966 0 |

Figure 4. Solution of the matrix game in mixed strategies.

Solution in the mixed strategies makes it possible to determine the probability of the strategy choice by every of the players. For the obtained results the third threat of intruder is the most probable while the fourth measure concerning elimination of the threats seems to be the most efficient one. Solution of the game equal to 0.081 means the efficiency of the system safety of the office.

In the real situation the office operates in the conditions of multiple external threats and objective limitations concerning the number of the responsive techniques to these threats. In these conditions can appear the problem of the distribution of the procured resources according to the detected threat, but with the account of characteristics of these threats. This problem can be solved with the application of the cooperative game theory.

\[ F_i(v) = \sum_{S \subseteq Z} \frac{(|S|-1)!(n-|S|)!}{n!} [v(S) - v(S \setminus \{i\})] \]  
\tag{4}

According to this theory basing on the idea of Shepley vector it is possible to obtain a single distribution of a certain resource over multiple objects.

Let us formulate statement of the problem for the application of the cooperative games theory. Suppose that a certain number of intruders are acting against a certain institution. Each of the intruders has a certain arsenal of tools, where their characteristics can be defined similar to the data in Table 1. The office has a certain number of countermeasures specified by the analogy with Table 3. It is necessary to determine the distribution of the office’s means over the intruders, taking into account the parameters that characterize them. As a result of solution of the problem certain measures can be determined, which are necessary for the realization relative to each of the intruder.

In this variant of the problem’s statement the problem can not be solved with the use of the matrix games theory since it allows considering the interaction only between two participants.
Practical application of the cooperative games theory requires a separate thorough consideration and it is not a subject of consideration in this publication.

4. Conclusion
All of the applications presented in the work allow to make a conclusion on the possibility of the use of the game theory to the problem of a system protection assessment.

Of course, the considered examples are simplified since in a number of cases the strategies can have considerably greater number of parameters. Increase of the problem size does not lead to appearance of the complications connected with the applying of group-theoretical approach. This open up possibilities for the practical realization of the obtained model in the form of a software, which can be utilized by the employees for analysis of the protection state in the office. The ways of formalization of linguistic constructions are not too complicated for their realization in software.

It should be also noted that matrices of the game interaction can be obtained not only for the pair of «threats-measures», but also for the pairs of «threats-vulnerabilities» and «vulnerabilities-measures». All of these pairs make it possible to analyze the state of the system safety from different points. It allows to get a complete pattern of the office protection. Moreover, for all the considered examples game matrices were formed on the basis of integrated assessment of the safety aspects. The variant of formation on the basis of specified parameters can be useful as well. For example, this may be realized on the basis of disruptiveness for the threats or within the set of measures providing office safety with a high efficiency.

References
[1] Menzhulin R and Moiseev S 2011 Management of efficiency of information protection in distributed payment systems based on bank cards Bulletin of Voronezh State Technical University (VGTU) 7(7) pp 95-8
[2] Stepanov L 2017 Concept of providing the information safety in telecommunication networks basing on the artificial immune systems Actual Problems of Applied Mathematics, Informatics and Mechanics: Collected Articles of the International Theoretical and Practical Conference pp 898-909
[3] Stepanov L 2019 Aspects of the application of the game theory to formalization of the Actual Problems in the Activity of FSIN Sub pp 93-6
[4] Stepanov L 2017 Formalization of the threats of the information safety and complex assessment of the information safety Bulletin of Voronezh Institute at FSIN of Russia 4 pp 156-162
[5] Belokurov S, Kuzmenko R, Moiseev S and Okuneva E 2016 Multi-criteria assessment of the objects safety of infocommunication systems with the account of latent parameters Bulletin of Voronezh Institute at Federal Penitentiary Service (FSIN) of Russia 4 pp 39-45
[6] Kuzmenko R and Moiseev S 2016 Simulation of efficiency of the information safety basing on Rasch model for the assessment of latent variables Collected Materials of All-Russian Theoretical and Practical Conference “Actual problems of the Departments Activity of Penitentiary System pp 253-4
[7] Dyubin G and Suzdal V 1981 Introduction to the applied game theory Vorobiev -Moscow: Nauka 336 p