Evaluating the Effectiveness of an Intrusion Detection System Based on Matrix Games and Fuzzy Sets

V B Vilkov¹, A I Dergachev¹, A K Chernykh¹, M S Abu-Khasan¹

¹Emperor Alexander I St. Petersburg State Transport University, St. Petersburg.

E-mail: pgups1967@mail.ru

Abstract. We consider a problem formulated as a matrix game in which the gain of officials using a specific intrusion detection system (criminal actions) of intruders (player 1) is the probability of timely detection of these criminal actions (player 2). As a rule, it is not possible to unambiguously set the probability of timely detection of criminal actions, so it is proposed to use the apparatus of fuzzy set theory to evaluate it. Reviewed and discussed the basic concepts of fuzzy set theory, and an example of practical application of this theory to assess the efficiency of the detection system of criminal damage. Application of fuzzy set theory in assessing the possible actions of an attacker can detect existing vulnerabilities in information security of automated systems continue to spend improving the detection of criminal acts (hackers) to prevent the possibility of applying economic and other damage to the company.

1. Introduction
Evaluation of the effectiveness of the use of intrusion detection systems and criminal actions of intruders in modern automated systems is currently a very urgent task.

This article deals with the problem formulated as a matrix game [1], in which the gain of officials using a specific intrusion detection system (criminal actions) of intruders (player 1) is the probability of timely detection of these criminal actions (player 2). As a rule, it is not possible to unambiguously set the probability of timely detection of criminal actions, so it is proposed to use the apparatus of fuzzy set theory to evaluate it.

The basic concepts of the theory of fuzzy sets are considered and disclosed, as well as an example of the practical application of this theory for evaluating the effectiveness of using the system for detecting criminal actions of intruders.

The application of the theory of fuzzy sets [2-7] in terms of assessing possible actions of a malicious user allows us to detect existing vulnerabilities in the information security of an automated system, and further improve the systems for detecting criminal actions of intruders (hackers), preventing the possibility of causing economic and other damage to the company.

2. Basic concepts and definitions
Under the matrix game, we will understand the game of two participants, in which each of them has a certain number of options for their actions (strategies) [8-10]. Players simultaneously and independently choose their strategy. This choice of strategies clearly determines the winnings of the players, which in total are equal to zero.
Suppose that \( a_1, a_2, \ldots, a_m \) — the strategies of the first player, and \( b_1, b_2, \ldots, b_n \) — the strategies of the second player. The players’ choice of their strategies is called a situation. Under the situation \((i, j)\), we will understand the situation in which the first player chose the strategy \( a_i \), the second — \( b_j \). For game \( g \), the winning functions \( H_g(i, j) \) and \(-H_g(i, j)\), respectively, of the first and second players, are defined, correlating their winnings to each possible situation in the game; each player strives to maximize his winnings.

The payoff matrix of the first player \( (A_g) \) uniquely defines the game \( g \) and has the form

\[
A_g = \begin{pmatrix}
H_g(1,1) & H_g(1,2) & \ldots & H_g(1,n) \\
H_g(2,1) & H_g(2,2) & \ldots & H_g(2,n) \\
\vdots & \vdots & \ddots & \vdots \\
H_g(m,1) & H_g(m,2) & \ldots & H_g(m,n)
\end{pmatrix}
\]  

(1)

Players can guarantee themselves winnings equal to \( \max_{1 \leq i \leq m} \min_{1 \leq j \leq n} H_g(i, j) \) and \( \min_{1 \leq j \leq n} \max_{1 \leq i \leq m} H_g(i, j) \), respectively.

In the matrix game \( g \), a situation \((i_0, j_0)\) is called an equilibrium, or saddle point, if

\[
H_g(i, j_0) \leq H_g(i_0, j_0) \leq H_g(i_0, j)
\]

at \( 1 \leq i \leq m \) and \( 1 \leq j \leq n \).

The price of the game is called the winning of the first player in an equilibrium situation, and the strategies that form the saddle point are called optimal. It should be noted that not every game has a saddle point, which makes the approach proposed in the article relevant[11-14].

When solving different problems, we can not always say unequivocally that this object fully possesses (does not possess) properties inherent in the elements of this set. For example, consider the set of possible values for the probability of detecting intruders "the probability of detecting an attacker is large". About the probability of detecting an attacker of 0.8, we can not say unequivocally whether it is or is not an element of this set. This led to the need to create a theory of odd sets. Let’s give some definitions.

Fuzzy sets are defined on some ordinary set \( U \), called a universal set. This can be a lot of automated systems, a lot of criminal actions of intruders, a lot of matrix games, etc. A fuzzy set \( \hat{A} \) on a universal set \( U \) is a set of pairs \((\mu_{\hat{A}}(u), u)\), \( u \in U \), where \( \mu_{\hat{A}}(u) \) is the membership function that expresses the degree of membership of an element \( u \in U \) to the fuzzy set \( \hat{A} \). As a rule, it is assumed that the membership function takes values from the segment [0, 1].

The intersection of the fuzzy sets \( \hat{A} \) and \( \hat{B} \) given on \( U \) is called the fuzzy set \( \hat{C} = \hat{A} \cap \hat{B} \) with the membership function

\[
\mu_{\hat{C}}(u) = \min\{\mu_{\hat{A}}(u), \mu_{\hat{B}}(u)\}, \; u \in U,
\]

(3)

their union is a fuzzy set \( \hat{D} = \hat{A} \cup \hat{B} \) with the membership function

\[
\mu_{\hat{D}}(u) = \max\{\mu_{\hat{A}}(u), \mu_{\hat{B}}(u)\}, \; u \in U.
\]

(4)
Fuzzy sets in the case when the universal set is a numerical axis and functions whose membership is continuous and has a single maximum are called non-clear numbers. Often, when solving practical problems, triangular fuzzy numbers are used. A triangular fuzzy number \( \hat{D} \) is a triple \( (c, d, f) \), \( c < d < f \), of real numbers such that

\[
\mu_{\hat{D}}(u) = \begin{cases} 
\frac{u-c}{d-c}, & \text{if } u \in [c, d], \\
\frac{f-u}{f-d}, & \text{if } u \in [d, f], \\
0, & \text{otherwise.}
\end{cases}
\]  

(5)

The second number of the triple \( (c, d, f) \) is usually called the mode, or clear value, of the fuzzy triangular number \( \hat{D} \), \( \mu_{\hat{D}}(d) = 1 \).

Following the publications [15, 19], we introduce some concepts of fuzzy logic. The degree of truth of a fuzzy statement takes values from a closed interval [20].

The degree of truth of a fuzzy statement \( P \) is denoted by \( \mu(P) \).

The conjunction of fuzzy statements \( P \) and \( T \) is a logical operation, the result of which is a fuzzy statement \( P \land T \), for which

\[
\mu(P \land T) = \min\{\mu(P), \mu(T)\},
\]

(6)

disjunction \( P \lor T \) — a logical operation for which

\[
\mu(P \lor T) = \max\{\mu(P), \mu(T)\}.
\]

(7)

Consider the problem statement for a fuzzy matrix game.

3. Problem statement for a fuzzy matrix game

Let \( G \) be the set of all matrix games with \( m \) strategies for the first player and \( n \) strategies for the second player. We will consider \( G \) as a universal set on which non-distinct sets are given-fuzzy matrix games of \( \hat{g} \), that is, games in which the winnings are given by non-distinct triangular numbers

\[
\hat{D}_{ij}(\hat{g}) = (c_{ij}(\hat{g}), d_{ij}(\hat{g}), f_{ij}(\hat{g})).
\]

The membership function of a fuzzy game \( \hat{g} \) is denoted by \( \mu_{\hat{g}}(g), g \in G \). Due to the fact that the matrix game is uniquely determined by the payoff matrix, we assume that \( g = A_{g} \) and, consequently, \( \mu_{\hat{g}}(g) = \mu_{\hat{g}}(A_{g}) \).

Let \( \hat{g} \) be a fuzzy game given on \( G \), and the first player's winnings are fuzzy numbers

\[
\hat{D}_{ij}(\hat{g}) = (c_{ij}(\hat{g}), d_{ij}(\hat{g}), f_{ij}(\hat{g})), \quad i = 1, 2, ..., m, \quad j = 1, 2, ..., n
\]

with membership functions \( \mu_{ij}^{\hat{g}} \).

In accordance with the definition of conjunction in fuzzy logic, we have:
Consider a fuzzy matrix game $\hat{g}$ with a fuzzy payoff matrix $\hat{A}_{\hat{g}} = \left[ \hat{D}_{ij}(\hat{g}) \right]_{i,j=1}^{m,n}$ and a set of games for which situation $(i,j)$ is a saddle point. By $F^{ij}(\hat{g})$ we denote the set of matrices of wins of such games.

Let $A^ij(\hat{g}) \in F^{ij}(\hat{g})$ and $\mu_{\hat{g}}(A^ij(\hat{g})) = \max_{A \in F^{ij}(\hat{g})} \mu_{\hat{g}}(A)$.

The value of $\mu_{\hat{g}}(A^ij(\hat{g}))$ will be considered as the degree of reliability that the situation $(i,j)$ in the game $\hat{g}$ is a saddle point. The solution to the game $\hat{g}$ is the situation $(i,j)$, for which the reliability of being a saddle point is maximal.

The task of finding the described solution to the game is reduced to solving a number of mathematical programming problems. Here is a graphic approach to solving this problem for a meaningful example.

### 4. Example of using the graphical approach to solve the game problem

As part of the improvement of the automated transport process management system of JSC "Russian Railways", it is necessary to effectively use the system for detecting criminal actions of intruders in terms of violations of transport process management, which prevents four variants of criminal actions of hackers. Hackers have four strategies for malicious actions. As malicious actions of hackers aimed at violating the information security of this automated system, we will consider: analysis of network traffic (hereinafter $b_1$), DDOS attacks (hereinafter $b_2$), virus infection of data (further $b_3$) and password interception (hereinafter $b_4$). Officials using the system for detecting criminal actions of hackers (the first player) also have four strategies for preventing these actions (protection strategies), respectively: traffic encryption (hereinafter $a_1$), firewall protection (hereinafter $a_2$), anti-virus protection (hereinafter $a_3$), one-time password (encryption of the communication channel) (hereinafter $a_4$). Under their winnings, it is proposed to consider the probabilities of timely detection of the actions of hackers (the second player). We assume that the available information about these probabilities is not sufficient, and it is fuzzy and is given using fuzzy numbers $\{c_{ij}, d_{ij}, f_{ij}\}$ (their modes are shown in Table 1).

| Protection strategies | The strategy of hackers |
|-----------------------|-------------------------|
| $a_1$                 | 0.95, 0.60, 0.50, 0.65  |
| $a_2$                 | 0.60, 0.90, 0.60, 0.55  |
| $a_3$                 | 0.50, 0.65, 0.95, 0.70  |
| $a_4$                 | 0.50, 0.60, 0.65, 0.95  |

We note the existing feature of the solution of the given example, which consists in the fact that, by setting the winnings to fuzzy numbers, we can get as an answer a situation with a zero value of the membership function.

As an illustration of what has been said, let us consider several cases.
1. In the case of \( c_{ij} = d_{ij} - 0.05 \) and \( f_{ij} = d_{ij} + 0.05 \), the reliability that the situation is a saddle point is zero, which requires further explanation.

2. If \( c_{ij} = \max \{ d_{ij} - 0.2, 0 \} \) and \( f_{ij} = \min \{ d_{ij} + 0.3, 1 \} \), then the situations become the saddle points with the maximum reliability specified in Table 2.

Table 2. Reliability of saddle points (case 2).

| Protection strategies | The strategy of hackers |
|-----------------------|-------------------------|
|                       | \( b_1 \)   | \( b_2 \)   | \( b_3 \)   | \( b_4 \)   |
| \( a_1 \)             | 0,1         | 0,2         | 0,1         | 0,1         |
| \( a_2 \)             | 0,2         | 0,3         | 0,2         | 0,2         |
| \( a_3 \)             | 0,1         | 0,2         | 0,1         | 0,1         |
| \( a_4 \)             | 0,1         | 0,2         | 0,1         | 0,1         |

The solution is the situation (2,2), in this situation with a reliability of 0.3, the first player wins 0.76 (with a reliability of 0.3, the probability of detecting criminal actions is 0.76).

3. Consider several cases where \( [c_{ij}, f_{ij}] \) is the same and \( [c, f] \) is equal for any \( i \) and \( j \). In this case, as a solution to any such game, we will get some situation with reliability greater than zero.

3.1. In the case of 1, the minimum value for \( c_{ij} \) is 0.45, and the maximum value for \( f_{ij} \) is one. If we use the interval \([0.45, 1]\) as \([c, f]\), which, in our opinion, is not meaningless, then the situations become saddle points with the maximum reliability indicated in Table 3.

Table 3. The reliability of the saddle points (case 3.1).

| Protection strategies | The strategy of hackers |
|-----------------------|-------------------------|
|                       | \( b_1 \)   | \( b_2 \)   | \( b_3 \)   | \( b_4 \)   |
| \( a_1 \)             | 0,55        | 0,579       | 0,55        | 0,55        |
| \( a_2 \)             | 0,579       | 0,611       | 0,579       | 0,579       |
| \( a_3 \)             | 0,55        | 0,579       | 0,55        | 0,55        |
| \( a_4 \)             | 0,55        | 0,579       | 0,55        | 0,55        |

The solution is the situation (2,2), in which with a reliability of 0.611, the first player wins 0.725.

3.2. If we implement the scheme of case 2, then the interval \([0.3, 1]\) could be used as \([c, f]\). Then the situations become the saddle points with the maximum reliability indicated in Table 4.

Table 4. The reliability of the saddle points (case 3.2).

| Protection strategies | The strategy of hackers |
|-----------------------|-------------------------|
|                       | \( b_1 \)   | \( b_2 \)   | \( b_3 \)   | \( b_4 \)   |
| \( a_1 \)             | 0,608       | 0,636       | 0,608       | 0,608       |
| \( a_2 \)             | 0,636       | 0,666       | 0,636       | 0,636       |
| \( a_3 \)             | 0,608       | 0,636       | 0,608       | 0,608       |
| \( a_4 \)             | 0,608       | 0,636       | 0,608       | 0,608       |

The solution is the situation (2,2), in which with a reliability of 0.686, the first player wins 0.70.

4. As the winnings of the first player, consider not the probabilities, but the usefulness of situations for him. If we rely on the probabilistic approach used by D. von Neumann and O. Morgenstern to de-
termine utility, then utility lies in the interval $[0, 1]$, and then we may have more reason to believe that $[c, f] = [0, 1]$. 

5. Representation of a graphical approach to solving a problem

We present a graphical approach to solving the problem, considering case 3.2. and situation $(2,2)$.

To solve it, first, for each situation $(i, j)$, $i = 1, 2, 3, 4$, $j = 1, 2, 3, 4$, we need to find a game for which the value of the membership function is maximal among all such games for which the situation in question is the saddle point. And, secondly, choose the situation for which the found value of the membership function is the maximum.

Denote:

$$
\mu^l_{ij}(u) = \frac{u - c_{ij}}{d_{ij} - c_{ij}}, \quad c_{ij} \leq u \leq d_{ij} \quad \text{and} \quad \mu^r_{ij}(u) = \frac{f_{ij} - u}{f_{ij} - d_{ij}}, \quad d_{ij} \leq u \leq f_{ij}. 
$$  \tag{9}

Recall that in order for the situation $(i_0, j_0)$ was in equilibrium, it is necessary to win in this situation do not exceed the winnings in situations $(i_0, j)$, $j = 1, 2, 3, 4$ (on line) and was not less wins in situations $(i, j_0), i = 1, 2, 3, 4$ (by column).

Consider the situation $(2,2)$. To get from the game with the payoff matrix given in Table 1, a game in which the situation $(2,2)$ is an equilibrium situation, you need to change the winnings in the third row to non-decreasing and the winnings from the fourth column to non-decreasing. The gain in the situation $(2,2)$ may need to remain unchanged, may need to be increased, or may need to be reduced.

Let's construct the necessary graphs of functions $\mu^l_{12}(u), i = 1, 2, 3, 4$ and $\mu^r_{2j}(u), j = 1, 2, 3, 4$ (Fig. 1).

![Figure 1. Membership functions $\mu^l_{12}(u)$ and $\mu^r_{2j}(u)$.](image)

In Figure 1, the numbers indicate the following function graphs: $1 \rightarrow y = \mu^l_{12}(u); 2 \rightarrow y = \mu^l_{42}(u); 3 \rightarrow y = \mu^l_{32}(u); 4 \rightarrow y = \mu^l_{22}(u); 5 \rightarrow y = \mu^r_{24}(u); 6 \rightarrow y = \mu^r_{21}(u); 7 \rightarrow y = \mu^r_{23}(u); 8 \rightarrow y = \mu^r_{22}(u)$.

If the situation $(2,2)$ is equilibrium with a win in it equal to $b$, then on the abscissa axis there is a point with an abscissa (win in the situation $(2,2)$ with reliability 0), a greater win (with reliability 0) on the column and a smaller win (with reliability 0) on the row. On the abscissa axis, we find the segment
for which the specified inequalities are satisfied. In Figure 1, these are the points of the abscissa axis from 0,3 to 1.

Above this segment, we find a point that is the intersection point of the increasing and decreasing graphs. If there are several such points, choose the point with the minimum ordinate from them. The abscissa of this point gives the desired gain in the situation under consideration, and its ordinate is equal to the maximum reliability that this situation is equilibrium[21,22].

In the figure, the desired point lies at the intersection of the graphs of the fourth and fifth functions. Their equations, respectively, have the form:

\[ y = \frac{u - 0.3}{0.9 - 0.3}; \quad y = \frac{1 - u}{1 - 0.55}. \] (10)

Solving this system, we find \( y \cong 0.67, x \cong 0.70 \), therefore, the reliability of the fact that the situation (2,2) (DDOS attack by hackers — protection strategy — firewall) is a saddle point is 0.67, with this reliability, the equal value of the probability of detecting and preventing criminal actions is 0.70.

6. Conclusion
As a conclusion, we note that the advantage of the proposed approach is that any game has a solution in pure strategies, which cannot be said about the classical approach.

7. References
[1] Vilkov V B, Chernykh A K 2019 O podxode k resheniyu zadachi komplektovaniya podrazdeleniy lichny`m sostavom na osnove potokovogo algoritma Voprosy` oboronnoy tehniki. Seriya 16: Texnicheskie sredstva protivodejstviya terrorizmu. 1-2 (127-128) pp 29-37
[2] Flegontov A V, Vilkov V B, Chernykh A K 2020 Modelirovanie zadach prinятиya reshenij pri nechetkix isxdony`x danny`x: monografija (Sankt-Peterburg: Lan` ) p 332
[3] Vilkov V B, Chernykh A K, Flegontov A V 2018 Zadachi na grafax s nechetko zadanny`mi vesami: monografija (SPB.: Izd. RGPU im. A. I. Gercena) p 160
[4] Kofman A 1982 Vvedenie v teoriyu nechetkix mnozhhestv (M.: Radio i svyaz`) p 429
[5] Chernykh A K, Kozlova I V, Vilkov V B 2015 Voprosy` prognozirovaniya material`no-texnicheskogo obespecheniya s ispol`zovaniem nechyotkix matematicheskix modelej Problemny` upravleniya riskami v texnosferе 4(36) pp 107-117
[6] Vilkov V B, Flegontov A V, Chernykh A K 2018 Matematicheskaya model` zadachi o raspredelenii v usloviyax neopredelennosti Differential`ny`e uравнения и processь upravleniya 2 pp 180-191
[7] Chernykh A K, Vilkov V B 2016 Upravlenie bezopasnost`yu transportny`x perevozok pri organizatsiyi material`nogo obespecheniya sil i sredstv MChS Rossii v usloviyax chrezvy`chajnoy situacii Pozharovzry`v`obezopasnost` T 25 9 pp 52-59
[8] Rusanova E, Abu-Khasan M, Sakharova A 2019 The control waste of communal services IOP Conference Series: 2019 Earth and Environmental Science 272(2) 022109 DOI: 10.1088/1755-1315/272/2/022109
[9] Abu-Khasan M, Egorov V, Rozantseva N, Kuprava L 2018 Load carrying wood and metal structures of trusses of covering of long spanned rail depot 2018 IOP Conference Series: Materials Science and Engineering 463(4) 042075 DOI: 10.1088/1757-899X/463/4/042075
[10] Maslennikova L, Abu-Khasan M, Babak N 2017 The use of oil-contaminated crushed stone screenings in construction ceramics Procedia Engineering 189 pp 59-64 DOI: 10.1016/j.proeng.2017.05.010
[11] Komokhov P, Maslennikova L, Makhmad A 2003 Control of strength of ceramic materials by forming the contact zone between clay matrix and leaning agent Stroit`lene Materi-aly 12 pp 44-46 ISSN: 0585430X
[12] Abu-Khasan M, Solovyova V, Solovyov D 2018 High-strength Concrete with new organic mineral complex admixture 2018-MATEC Web of Conferences 193 03019 DOI: 10.1051/matecconf/201819303019
[13] Rusanova E, Abu-Khasan M, Egorov V 2020 Influence of wooden cross ties on the surrounding medium at operation of transport objects in cold regions IOP conference series: materials science and engineering C 022042 DOI: 10.1088/1757-899X/753/2/022042
[14] Rusanova E, Abu-Khasan M, Egorov V 2020 The complex evaluation of geo eco-protective technologies taking into account the influence of negative temperatures IOP conference series: materials science and engineering 022042 DOI: 10.1088/1757-899X/753/2/022042
[15] Dergachev A, Dergachev S, Perepechenov A, Abu-Khasan M 2019 Fundamentals of Algorithmization of Functional and Computational Problems 2019 International Multi-Conference on Industrial Engineering and Modern Technologies FarEastCon 2019 8933942 DOI: 10.1109/FarEastCon.2019.8933942
[16] Veselov V, Abu-Khasan M, Egorov V 2020 Innovative design of wooden beams in the far North IOP conference series: materials science and engineering DOI: 10.1088/1757-899x/753/2/0220242
[17] Abu-Khasan M, Rozantseva N, Egorov V, Kuprava L 2020 Prefabricated Dome Structures with Walls Made of Soil Composites and Urea-Formaldehyde Foam Insulation (UFFI) as a Way to Solve Transport Infrastructure Problems in Permafrost Regions IOP conference series: materials science and engineering 022022 DOI: 10.1088/1757-899X/753/2/022022
[18] Temnev V, Abu-Khasan M, Charnik D, Kuprava L, Egorov V 2020 The mesh of shells of a bionic type to be operated in extreme habitats IOP conference series: materials science and engineering 022023
[19] Egorov V, Kravchenko A, Abu-Khasan M 2020 The Application of Evolutional Algorithm Optimization of Sprengel Systems of Transport Buildings and Structures for Northern Districts IOP conference series: materials science and engineering 022020 DOI: 10.1088/1757-899X/753/2/022020
[20] Egorov V, Abu-Khasan M, Shikova V 2020 The systems of reservation of bearing structures coatings of transport buildings and constructions for northern areas IOP conference series: materials science and engineering 022021 DOI: 10.1088/1757-899X/753/2/022021
[21] Abu-Khasan M, Egorov V 2020 The Influence of Different Types of Reinforcement on the Deformation Characteristics of Clay Soil in the Conditions of Seasonal Freezing and Thawing IOP conference series: materials science and engineering 022041 DOI: 10.1088/1757-899X/753/4/042083
[22] Chernykh A K, Gorshkova E E, Dergachev A I, Abu-Khasan M S Use of Integrated Accounting Methods for Calculation of the Profile Volume of Embankments IOP Conference Series: Earth and Environmental Science DOI:10.1088 / 1755-1315 / 459/6/062008
[23] Vilkov V B, Dergachev A I, Chernykh A K, Abu-Khasan M S 2020 On the Concept of Solving a Fuzzy Cooperative Game with Side Payments International Multi-Conference on Industrial Engineering and Modern Technologies FarEastCon 2020 9271558 DOI: 10.1109/FarEastCon50210.2020.9271558