ISSN 2278-3091
Volume 9, No.4, July – August 2020
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse124942020.pdf
https://doi.org/10.30534/ijatcse/2020/124942020

Adaptive Model of Cybersecurity Financing with Fuzzy Sets of Threats and Resources at the Protection Side

Akhmetov B.S.[1], Lakhno V.A.[2], MalyukovV.P.[3], Doszhanova A.A.[4], AlimseitovaZh.K.[5]
[1]Kazakh National Pedagogical University named after Abay, Department of Education Informatization, Almaty, Kazakhstan, bakhytzhan.akhmetov.54@mail.ru
[2]National University of Life and Environmental Sciences of Ukraine,Department of Computer systems and networks, Kyiv, Ukraine, lva964@gmail.com
[3]National University of Life and Environmental Sciences of Ukraine,Department of Computer systems and networks, Kyiv, Ukraine,volod.malyukov@gmail.com
[4]Gumarbek Daukeev Almaty University of Energy and Communications, Department of IT Engineering, Almaty, Kazakhstan, a.doszhanova@aues.kz
[5]Gumarbek Daukeev Almaty University of Energy and Communications, Department of IT Engineering, Almaty, Kazakhstan, zhuldyz_al@mail.ru

ABSTRACT

The article proposes an adaptive model for selection of strategies for cybersecurity financing of an informatization object with incomplete information on the financial resources of the attacking side. The case is considered when the financial resources of the protection side belong to some fuzzy set. The model is intended for the developed decision support system in the tasks of selection of rational variants for investing in information protection systems. The solution was obtained by using the tools of the theory of multi-step games with several terminal surfaces. The model is distinguished by the assumption that the protection side does not have complete information both about the financial strategies of the attacking side and about the state of its financial resources aimed at overcoming the boundaries of information protection. The assumption is made that the protection side has the opportunity to obtain additional information due to spending a part of its financial resources. The model was tested using a computational experiment, the results of which are also given in the article.

Key words: Decision support system, game theory, information protection, informatization object, financial strategy, fuzzy sets.

1. INTRODUCTION

Nowadays, almost any informatization object (IO) needs to protect its information resources. Already at the design stage, for almost all IOs and their information systems (IS), funds are allocated to the budget for the creation or modernization of appropriate information protection systems (IPS) and cybersecurity (CS). Moreover, we should note that the more complex the informatization object, for example, if we compare the protection of the university information system [1] of the bank [2], the respectively more cyber security circuits must be on the protection side [3], [4]. Modern IPS and CS are multi-layered complexes, including antivirus software, firewalls, systems for detecting attacks and anomalies in the network, cryptographic applications, etc. [1], [3], [4].

We also note that, as cyber attack scenarios become more complex on IO or critically important computer systems (CICS), it is difficult for the protection side to form in advance the hardware-software component of complexes and circuits of IPS based on traditional strategies for selecting cybersecurity tools and systems. And it may well be a real situation in which the protection side needs to dynamically take into account the landscape changes of cyber threats, which automatically leads to the need to revise or reconfigure the IO protection circuits. And this, in turn, is associated with additional financial costs, for example, for the acquisition of new firewalls, intrusion detection systems and etc. In the context of the blurring of cyber threats and the existing tendency for the occurrence of new threats and attack scenarios, we can say that solving the problem of selection of the financial component of the strategy to counter cybercriminals is a dynamic task. And while in real situations, we can say that a lot of resources on the protection side correspond to certain fuzziness of the parameters.

As it is known, in most cases, the classes of objects found in the real physical world do not have a well-defined membership criterion. Moreover, an indisputable fact is that such inaccurately defined “classes” play an important role in human thinking, in particular, in such areas as computer science, cybernetics, artificial intelligence, pattern recognition, information transfer and abstraction, and others.

It should be noted that the concept of a fuzzy set provides a convenient starting point for the creation of conceptual foundations that are parallel in many respects to the foundations used in the case of ordinary sets, but more general than the last ones and potentially have a wider scope. In particular, this applies to areas such as: pattern classification; data processing; game theory, etc. It is significant that such foundations provide a natural way to solve problems in which the source of inaccuracy is more likely the absence of clearly defined criteria for class membership than the presence of random variables. Therefore, this article attempts to solve problems of a conflicting nature and in which the incompleteness of the

information is not stochastic, but has the nature of fuzzy information defined by fuzzy sets.

In [4]–[6], there was shown that one of the main problems in creation of integrated IPS and CS is the choice of a rational investment strategy in IPS and CS for IO. The trend in recent years on the intellectualization of decision support [6, 7] in the field of IO cyber security tasks has made it possible to take a fresh look at the unsolved problems for such systems. In particular, the problem of developing new models for the selection of rational strategies for financing IPS and CS remains actual. For example, this is necessary in situations where the protection side may face new hacking technologies. This, in turn, changes the levels of cyber risks for IO. Therefore, as a result, a situation may potentially arise when the protection side needs to revise its strategies of financing in IPS and CS in order to choose a rational one.

2.THE PURPOSE OF THE ARTICLE

Is to develop a model for decision support systems for selection of rational strategies for financing cyber protection of an informatization object.

3.LITERATURE REVIEW

The most common model in practical application was proposed by American researchers Lawrence Gordon and Martin Loeb in 2002 [3]. The work describes an economic model that determines the optimal amount of investment to protect a given set of information. The model takes into account the vulnerability of information for a security hack and the potential loss in case of such a hack. Let note that the structure of the model is static - decisions and results occur simultaneously, and dynamic effects, including the dependence of money on time, are not taken into account.
Despite the fact that the Gordon – Loeb model after publication was recognized in the scientific community and supplemented by both other authors [4], [5], [6] and Lawrence Gordon and Martin Loeb themselves [7], many issues still have to be resolved. An indisputable fact is that the authors of the model for the first time thoroughly examined the problem and identified the vulnerability function, which is a key indicator of information security.

VuchenSchim, based on the work of Gordon-Loeb [3], developed his own model of interrelated risks for two identical enterprises [8]. The author has demonstrated that the optimal number of investments in cybersecurity with negative external effects will be greater than or equal to the optimal number of investments with independent risks, and the area of zero investments will be less. If cooperation between enterprises creates positive external effects, then the optimal number of investments in cybersecurity will be greater than or equal to the optimal number of investments with independent risks, and the area of zero investments will be identical to the model with independent risks.

In works [8]–[10], there was substantiated the need for the use of computer decision support systems (DSS) for solving investment project selection tasks in IPS. This is due to the rather large amount of initial data and iterative procedures for selection of rational investment strategies in IO protection systems.

In [8]–[10], the methodologies for creating various modules for the DSS in the field of financing IPS and for IS for various purposes were described in sufficient detail. One of the disadvantages of the analyzed works is the lack of models for selecting strategies for investing IPS, in situations where the protection side does not have complete information about the financial resources (FR) of the attackers. In [11] it was shown that this is an important characteristic of the attacking side. Since this indicator that ultimately allows to understand the potential of hackers. Indeed, the financial resource even of a powerful hacker group and the resource of a cyber-military side of a potential intruder can differ significantly [3].

Our new study develops the ideas previously expressed by the authors in [12], [13]. In the framework of the previously proposed scheme for selecting financing strategies of IPS, based on game theory. In accordance with similar works, which are also based on theory [14], [15], two sides are considered: player No.1 – information protector (INP); player No.2 – a hacker. Both players use FR to achieve their goals [13], [16]. Let note that in the analysis of the available approaches, we were not able to find conceptually similar publications. According to [13], [14], [16], the difference from a game with full information is that INP does not know exactly the initial financial state of the second player (hacker).

In view of the foregoing, it seems relevant to improve the models for the selection of rational strategies for financing IPS. The difference of this research is the introduction of variables into the model that take into account the fuzziness of information on the financial resources of the protection side. And, accordingly, of the variables providing the need to finance the procedure for obtaining additional information by the protection side by spending a part of its resources.

4. MODELS AND METHODS

IO security is determined on the basis of damage that is associated with the implementation of cyber threats that are random in nature. At the same time, hazard coefficients are correlated with specific parameters of IPS. And one of these parameters is the price-quality ratio of IPS. At the same time, these parameters, or their combination, are represented by fuzzy values, and the IO security indicator is determined by the matrix of fuzzy relationships between the hazard coefficient of the set of threats and the degree of security of the IO. The approach to assessing the effectiveness of technical information protection tools (TIPT) in IO is based on a comparative analysis of security indicators without the use of TIPT and with their application. At the same time, we are talking about the conditions of a fuzzy representation of the degree of danger of anthropogenic and technogenic threats to IO. With the increasing complexity of the objects of analysis, the composition and characteristics of threats (first of all, we are talking about threats of unauthorized remote access), the task of quantity assessment of the security of IO and CICS is relevant. Assessment of the effectiveness of TIPT is possible on the basis of such approaches: 1) comparison of the value of the security indicator with the normative (threshold); 2) comparison of information security indicators without TIPT and with TIPT.

Both approaches are applied at the level of particular models and techniques. For a comprehensive assessment of effectiveness, the first approach is not acceptable, because it is difficult to determine the acceptable levels of reducing the security of IO and CICS from a complex of modern cyber threats. The second approach is applicable in a comparative analysis of the effectiveness of measures and IPS and does not allow to determine the sufficiency of TIPT.

With the increasing complexity of IO, the change in the set and nature of IS and CS threats, especially threats of unauthorized remote access to resources and processes in CICS, the task of quantity assessment of the security is relevant. A correct assessment of the CICS security and the development of the financial component of the cyber protection strategy of IO and CICS is necessary to perform a comparison of similar systems in purpose and complexity, or to monitor the dynamics of the level of security of a specific IO in time.

Solving practical problems, there is applied the procedure of successive approximation of the model of the problem under consideration to the real one. Accordingly, based on the solution of the problem within the framework of a simpler model, we can find a solution to the real problem - the definition of a rational strategy for financing IO protection systems.

For example, in [13], [17] there were considered situations when the sets of preferences of the first player and his optimal strategies were found. This meant that if the states of the players belong to the sets of preferences of the first player, then he has a strategy, the implementation of which will allow him to achieve his goal. Thus, with a given probability, player No.1 (i.e., information protector – INP) put the system into a state that reflects a positive result for him. However, there may be situations where the protector needs to get a positive result for him from states from which he cannot make at the standard setting of the game rules. For example, he is limited in interaction time. Then it seems appropriate to introduce a procedure for obtaining additional information by spending a part of his resources for its obtaining. This procedure is especially relevant in case when the information incompleteness is either stochastic or has the nature of fuzzy information. At the same time, it should be noted that fuzzy information is typical in real life. So, in case of expert assessments, the fuzziness of expert opinions is inevitable, which requires the development of tools to solve such problems, especially when the uncertainty caused by the conflict situation is added. And, as practice has shown, one of the effective tools in such situations is the application of game theory.

4.1Results of Computational Experiments

The article considers the problem of financing an information protector in terms of his counteraction to the hacker side with the introduction of a subtask and the corresponding procedure for obtaining additional information. Additional information can be obtained by INP by spending apart of his resources for its obtaining. In contrast to similar researches, there is considered a situation when there is fuzzy information about the financial resources of the protection side.

4.2 Problem Solution

Both players require financial resources to achieve their goals. We assume that for a given period of time $\{0,1,...,\ T\}$ (T – natural number) INP allocates $x(0)$ financial resources (FR). The second player, respectively – $y^{\xi}(0)$. These resources determine the predicted, at the moment of time $t=0$, value of the FR that players possess to achieve their goals. Players interact. This interaction will be described as a bilinear multi-step game (BMSG) with alternate moves with fuzzy information. Unlike a game with full information, INP does not exactly know the initial state of the second player. However, INP knows the information that the states of the second player belong to the fuzzy set $\{X, m(.)\}$, where the fuzzy set X represents the segment $[a-r, b+r]$, $a, b, r-$ positive numbers, $b \geq a,\ a \geq r,\ b-a \geq 2\times r$ and the membership function $m(.)$is defined as follows:

$$m(x)=\begin{cases} 0, & x \leq a-r, \\ \left(\frac{1}{2\times r}\right)\times(x-a+r), & a-r \leq x \leq a+r, \\ 1, & a+r \leq x \leq b-r, \\ \left(-\frac{1}{2\times r}\right)\times(x-b-r), & \\ 0, & x \geq b+r \end{cases}. \quad (1)$$

Also the first player knows:

1) the initial state and parameters that determine the interaction of the parties;

2) all his states $x(\tau)$ for $\tau \leq$ t.

It is assumed that the first player (INP) can receive additional information by spending a part of his FR. It turns out as a result of introducing a parameter $k(k \in [0,1])$ that determines a part of the resource of the first player. This part of the FR is equal to $(1-k)\cdot z$. We assume that $z-$ the value of the INP resource, which is used to obtain information. This additional information concerns the state y^{ξ} of the second player (hacker) and belongs to the fuzzy set $\{Y, m(.)\}$, where $Y=[a-k^2\cdot r, b+k^2\cdot r]$, $a, b, r-$ positive numbers, $b \geq a,\ a \geq r,\ b-a \geq 2\times r.$ The membership function m(.) is defined as follows:

$$(x)=\begin{cases}0, & x\le a-k^2\cdot r,\\ \left(\frac{1}{2\times k^2\cdot r}\right)\times\left(x-a+k^2\cdot r\right), & a-k^2\cdot r\le x\le a+k^2\cdot r,\\ 1, & a+k^2\cdot r\le x\le b-k^2\cdot r,\\ \left(-\frac{1}{2\times k^2\cdot r}\right)\times\left(x-b-k^2\cdot r\right), & \\ 0, & x\ge b+k^2\cdot r\end{cases}. \quad (2)$$

Reasoning is carried out from the position of the first player (i.e. INP). Therefore, no assumptions are made about the awareness of the second player (hacker). Players take steps in turn. In even moments, the first player takes a step, in odd moments - the second one.

Let $t=2n$ and $x(t),\ x(t+1)-$ the states of the first player at the moment of time $t, t+1$. Also $y^{\xi}(t),\ y^{\xi}(t+1)-$ the states of the second player at the moment of time $t, t+1$. Then the states of the players at the moment of time $t+1, t+2$ are determined from the relations:

$$x(t+1)=k(t)\cdot\alpha\cdot x(t)-u(t)\cdot k(t)\cdot\alpha\cdot x(t);$$
$$y^{\xi}(t+1)=y^{\xi}(t)-s_1\cdot u(t)\cdot k(t)\cdot\alpha\cdot x(t); \quad (3)$$

$$y^{\xi}(t+2)=\beta\cdot y^{\xi}(t+1)-v(t)\cdot\beta\cdot y^{\xi}(t+1);$$
$$x(t+2)=x(t+1)-s_2\cdot v(t)\cdot\beta\cdot y^{\xi}(t+1); \quad 4)$$

Here

$$u(t), v(t), k(t): u(t)\in[0,1],\ v(t)\in[0,1], k(t)\in[0,1];\ s_1>0, s_2>0.$$

Let define the function:

$$F(.): R\to R,\ F(x)=\{\sup m(y),\ for\ y\le x\}. \quad (5)$$

Let denote by $\{X_t, m_t(.)\}, (t=0,1,...)$ the fuzzy sets to which the states of the second player belong for the so-defined dynamics of the players states; by

$$F_t(.): R\to R,\ F_t(x)=\{\sup m_t(y),\ for\ y\le x\}.$$

A detailed description of the game was given by us in [12], [13]. Therefore, in the framework of this article, we focused on considering the situation when, after the attacker (hacker) makes a move, the condition $x\cdot(t+2)>0$ will be satisfied with confidence of less than $p_1, (0\le p_1\le 1)$. That is, we can say that the hacker caused damage to IS with reliability more than $(1-p_1)$. Then the procedure for financing cybersecurity tools for this configuration of protection barriers is over. Otherwise, the procedure continues.

As in [12], [15], the first player seeks to find many of his initial states (InS), which have the following feature.

Feature: if the game starts from InS, then the first player can choose his control actions $u(0), k(0),.., u(t), k(t)\ (t=2n)$ to protect his IS with confidence more than p_0. Moreover, INP is able to prevent damage by a hacker with confidence more than $(1-p_1)$. The set of such states will be called the set of preferences of the first player.

At the same time, the strategy of the INP is a rule that allows to determine the amount of FR, on the basis of available information, that are spent on the development of cyber security systems. Also, a part of the funds was used to obtain additional information about the second player (hacker). The second player chooses his strategy $v(.)$ based on any information.

The goal of the first player is to find his set of preferences. INP strategies are also determined, applying which he will receive the fulfillment of conditions allowing him to complete the procedure for financing cyber protection. The strategies of the first player with the specified features will be called his optimal strategies.

The formulated game model corresponds, according to the classification of decision theory, to the problem of decision making in the conditions of fuzzy information. Let note that such a model is a nonlinear multi-step quality game with several terminal surfaces with alternate moves.

It should be noted that finding the sets of preferences of the first player (INP) and its optimal strategies depends on many parameters.

Taking into account the works [13], [15], [19] of the player's set of preferences for a situation where the protection side has resources that are described by a fuzzy set and it uses the procedure for obtaining information at the first step, the following expressions were obtained.

We give a case $p_1 = p_0$.

The set of preferences of the first player at the step T for the case using the additional information procedure at the first step will be denoted by $V^T_{1,k(1)}(p_0, p_0)$.

Since in [13], [15], [19], [20] a record of optimality sets and optimal strategies of players is given, in this article we present a record of these sets and optimal strategies for the simplest case.

$$T=1.$$

At $p_0: 0\le p_0\le 0{,}5$ we obtain $V^1_{1,k(1)}(p_0, p_0)=\varnothing.$

At $p_0: 0{,}5<p_0<1$ we obtain:

If $a<2\cdot p_0\cdot r-r$, then

$$V^1_{1,k(1)}(p_0, p_0)=\left\{\begin{matrix}x(0): 2\sqrt{a(2\cdot p_0\cdot r-r)}\le \\ \le s_1\cdot\alpha\cdot x(0)<a+2\cdot p_0\cdot r-r\end{matrix}\right\},$$

Optimal strategy of INP is a couple of functions $[u(.,.,.), k(.,.,.)]$:

$$\left(\bar{k}(1)\right)_2<k^*(x(0), F(.))<(k(1))_1,$$

$$\left(\bar{k}(1)\right)_{1,2}=\frac{s_1\cdot\alpha\cdot x(0)\pm\sqrt{(s_1\cdot\alpha\cdot x(0))^2-4\cdot a(2\cdot p_0\cdot r-r)}}{2\cdot(2\cdot p_0\cdot r-r)}; \quad (6)$$

$u^*(x(0), F(.)) = 1;$ at $x(0): 2 \cdot \sqrt{a \cdot (2 \cdot p_0 \cdot r - r)} \le s_1 \cdot \alpha \cdot x(0).$ (7)

$u^*(x(0), F(.)) = 0;;$ at $x(0): s_1 \cdot \alpha \cdot x(0) < 2 \cdot \sqrt{a \cdot (2 \cdot p_0 \cdot r - r)}.$ (8)

At $a \ge 2 \cdot p_0 \cdot r - r$ we obtain $V^1_{1,k(1)}(p_0, p_0) = \varnothing.$

It should be noted that the task of the fuzzy set in the form of a segment is not a big limitation introducing the procedure for obtaining additional information. It is enough to limit ourselves, for example, to the "left side" of the segment, which will not affect the determination of optimality sets and optimal strategies of players.

5.COMPUTATIONAL EXPERIMENTS

The effectiveness and adequacy of the model developed in the work was confirmed by experiments. In the experiments, there were set the tasks to determine the sets of strategies of the players of both the protection and the attacking sides and, in addition, to check the adequacy of the mathematical model.

Below there are the results of three computational experiments, which are presented on Figures 1–3. Cases 1–3 correspond to these experiments.

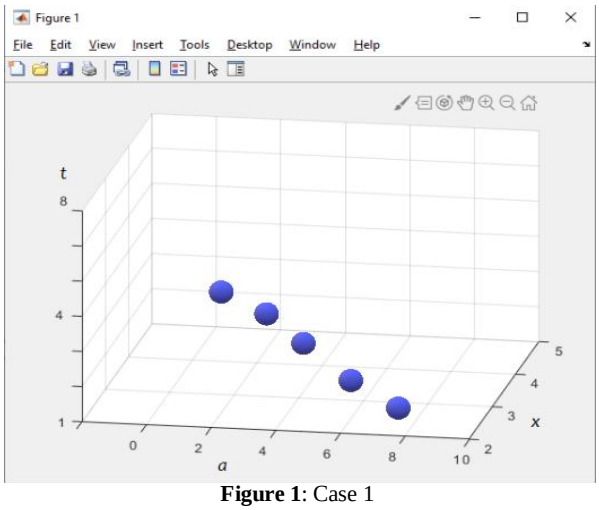

Figure 1: Case 1

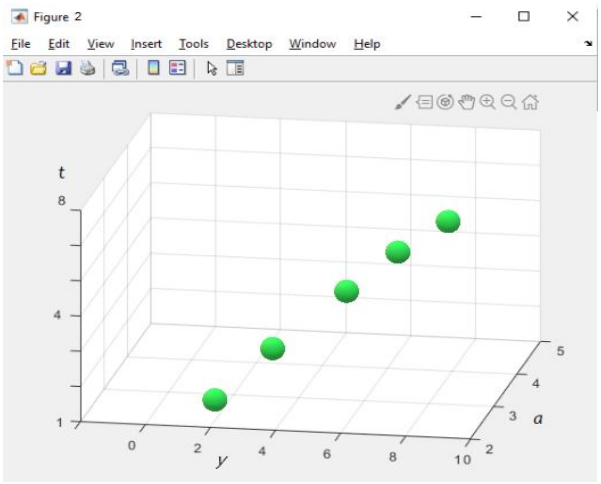

Figure 2: Case2

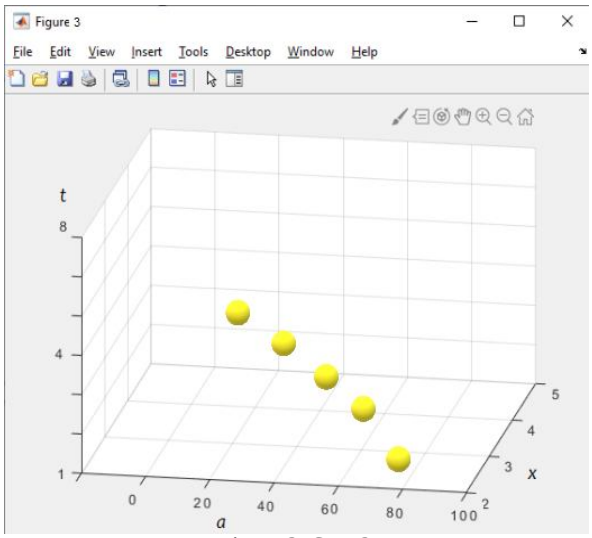

Figure 3: Case 3

Three cases are given. However, it should be noted that solutions are obtained for all cases of the correlation of game parameters. The results obtained using the model considered in the work made it possible to find the optimal financial strategies for the protector of the informatization object for any ratio of interaction parameters.

The maximum deviation of the results of a computational simulation experiment from practical data was 9–12%.

6.DISCUSSION OF SIMULATION RESULTS

Three-dimensional positive orthant in three-dimensional space $(t, x(0), a)$ is considered. The time axis t "goes from bottom to top, from zero". The parameter t means the number of steps of the players.

Test calculation No.1 (Figure 1). The following trajectory is obtained: (0, x(0), a(0))) = (0, 3, 6.5), (1, x(1), a(1)) = (1, 3.5, 5.5), (3, x(3), a(3)) = (3, 4.0, 5.0), (5, x(5), a(5)) = (5, 4.5, 4.0), (7, x(7), a(7)) = (7, 5.0, 3.0). Let note that points are considered in three-dimensional space $(t, x(0), a)$.

The Figure 1 shows the trajectory of the state movement of the dynamic system, which describes the positions of the players at the corresponding time instants. At each moment of time, the state of the system is described on Figure 1 by a "blue ball". When players apply optimal strategies, the state of the system approaches the terminal set, which is preferable for the first player.

Test calculation No.2 (Figure 2). For the set of preferences of the second player (attacking side), there is consideredsymmetric problem.

The following trajectory is obtained:(0, a(0), y(0)) = (0, 5.0, 3.0), (1, a(1), y(1))=(1, 4.0, 4.0), (3, a(3), y(3))=(3, 3.0, 5.0), (5, a(5), y(5))=(5, 2.0, 6.0), (7, a(7), y(7))= (7, 1, 8.0). At each moment of time, the state of the system is described on Figure 2 by the "green ball". When players apply optimal strategies, the state of the system approaches the terminal set that is preferable for the second player.

Test calculation No.3 (Figure 3). Corresponds to the "movement" along the line of balance.

Here we consider the initial task for the first player. The following trajectory is obtained:(0, $x(0)$, $a(0)$) = (0, 5, 75.0), (1, $x(1)$, $a(1)$)=(1, 4, 48.0), (3, $x(3)$, $a(3)$)=(3, 3, 27.0), (5, $x(5)$, $a(5)$) = (5, 2, 12.0), (7, $x(7)$, $a(7)$) = (7, 1, 3.0).

At each moment of time, the state of the system is described on Figure 3 by a "yellow ball". When players apply optimal strategies, the state of the system "moves" along the line of balance.

Therefore, computational experiments confirmed the adequacy of the refined model in case when there is fuzzy information about the state of the counterparty of financial interaction. Also there is confirmed the ability of the model to provide effective decision support with fuzzy information in the field of cybersecurity financing of various IOs. The work continued a number of publications of the authors [8], [12], [13], in which there were presented the theoretical and methodological foundations of the DSS design with different variants for awareness of the parties. This work develops these researches in the framework of complementing the existing DSS [13], [15] with mathematical models that are based on a BMSG with several terminal surfaces [15], [18]. Clarifications in the model regarding the information security of the parties, which allow a more adequate description of real situations, eliminate the disadvantages of the solutions described in [8], [13], [19]–[30]. For example, in [8], [13], all the initial conditions for selection of financial strategies for investing in cyber protection of IOs were not taken into account.

7.GRATITUDES

The research and the article were done within the framework of promising scientific and technical programs of the Department of Computer Systems and Networks of the National University of Life and Environmental Sciences of Ukraine, as well as the grant of the Republic of Kazakhstan, registration number AP05132723 "Development of adaptive expert systems in the area of cybersecurity of critical objects of informatization".

8. CONCLUSIONS

There were proposed additions to the models describing the procedures for financing the cybersecurity system of informatization objects. In contrast to existing solutions, there is considered the case when the protection side does not have complete information both about the financial strategies of the attacking side and about the states of his financial resources aimed at overcoming the boundaries of protection of the informatization object. In this case, the protection side has the opportunity to obtain additional information by spending a part of his financial resources. The solution is given for the case when the financial resources of the protection side are described using a fuzzy set. The solution is based on the dynamic programming method. In order to find solutions, there was used the apparatus of a non-linear multi-stage quality game with several terminal surfaces with alternate moves.

The results of a computational experiment are presented. In the process of simulation modeling and the selection of rational financial protection strategies, the operability of the model, as well as its adequacy, was confirmed. The deviation of the results of the computational experiment from practical data did not exceed 12%

REFERENCES

1.C.Posey, T.Roberts, P.Lowry, B.Bennett, J. Courtney,***Insiders' protection of organizational information assets: Development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors,*** 2013.

2.C.Posey, T. L.Roberts, P.B. Lowry, R.T. Hightower, **Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders,***Information & management*, no. 51(5), pp. 551–567, 2014.

3.R.W.Taylor, E.J. Fritsch,J.Liederbach, ***Digital crime and digital terrorism,*** Prentice Hall Press, 2014.

4.L.A.Gordon, M.P.Loeb, L.Zhou, **Investing in cybersecurity: Insights from the Gordon-Loeb model**, *Journal of Information Security*, no. 7(02), p. 49, 2016.

5.B.B. Kelly, **Investing in a centralized cybersecurity infrastructure: Why hacktivism can and should influence cybersecurity reform**,*BUL Rev.*, no. 92, p. 1663, 2012.

6.K. Goztepe,**Designing Fuzzy Rule Based Expert System for Cyber Security**,*International Journal of Information Security Science*, vol. 1, no 1, pp. 13–19, 2012.

7.A. Fielder, E. Panaousis, P. Malacaria et al., **Decision support approaches for cyber security investment**, *Decision Support Systems*, vol. 86, pp. 13–23, 2016. DOI:10.1016/j.dss.2016.02.012

8.V. A. Lakhno, **Development of a support system for managing the cyber security**, *Radio Electronics, Computer Science, Control*, No. 2, pp. 109-116, 2017, DOI: 10.15588/1607-3274-2017-2-12

9.H. Cavusoglu, B. Mishra, S. Raghunathan, **A model for evaluating IT security investments**, *Communications of the ACM*, vol. 47, issue 7, pp. 87-92, 2004. DOI:10.1145/1005817.1005828

10.L.A.Gordon, M.P.Loeb, W.Lucyshyn, L. Zhou, **The impact of information sharing on cybersecurity underinvestment: a real options perspective**, *Journal of Accounting and Public Policy*, no. 34(5), pp. 509–519, 2015.

11.A. Fielder, S. Konig, E. Panaousis, S. Schauer, S. Rass, ***Uncertainty in Cyber Security Investments***, [Online]. Available: https://arxiv.org/abs/1712.05893

12.B.Akhmetov, V.Lakhno, Y.Boiko,A.Mishchenko, **Designing a decision support system for the weakly formalized problems in the provision of cybersecurity**, *Eastern-European Journal of Eenterprise Technologies*, no. (1 (2)), pp. 4–15, 2017.

13.V. Lakhno, V. Malyukov, N. Gerasymchuk et al., **Development of the decision making support system to control a procedure of financial investment**, *Eastern-European Journal of Enterprise Technologies*, vol. 6, issue 3, pp. 24-41, 2017. DOI: 10.15587/1729-4061.2017.119259

14. M. H. Manshaei, Q. Zhu, T. Alpcan et al., **Game theory meets network security and privacy**, *ACM Computing Surveys*, vol. 45, issue 3, pp. 1-39, 2013. DOI:10.1145/2480741.2480742

15.V.P. Malyukov, **Discrete-approximation method for solving a bilinear differential game**, *Cybernetics and Systems Analysis*, vol. 29, issue 6, pp. 879 - 888, 1993.

16.A. Fielder, E. Panaousis, P. Malacaria et al. **Game theory meets information security management**, in Proceedings of the *IFIP International Information Security Conference*, Marrakech, Morroco, 2–4 June 2014, Berlin, Springer, pp. 15-29.

17.X. Gao, W. Zhong, S. Mei, **A game-theoretic analysis of information sharing and security investment for complementary firms**, *Journal of the Operational Research Society*, vol. 65, issue 11, pp. 1682-1691, 2014. DOI:10.1057/jors.2013.133

18.R. Isaacs, ***Differential games: a mathematical theory with applications to warfare and pursuit, control and optimization***,*Courier Corporation*, 1999.

19.B. Akhmetov, V. Lakhno**System of decision support in weakly-formalized problems of transport cybersecurity ensuring**,*Journal of Theoretical and Applied Information Technology*, vol. 96, no. 8, pp. 2184–2196, 2018.

20.V. Lakhno et al. **Developing of the cyber security system based on clustering and formation of control deviation signs**, *Journal of Theoretical & Applied Information Technology*, vol. 95, no. 21, pp. 5778–5786, 2017.

21.K.H. Abdul-Rahman, S.M. Shahidehpour, **Application of fuzzy sets to optimal reactive power planning with security constraints**, *IEEE Transactions on Power Systems*, 9.2: pp. 589–597, 1994.

22.Kilic, Mesut; Kaya, İhsan. **Investment project evaluation by a decision making methodology based on type-2 fuzzy sets**, *Applied Soft Computing*, 27: pp. 399–410, 2015.

23.Gu, Xiang; Wang, Ying; Yang, Bei. **A method for hesitant fuzzy multiple attribute decision making and its application to risk investment**, *Journal of Convergence information technology*, 6.6: pp. 282–287, 2011.

24.Tang, Yu-Cheng, et al. **Application and development of a fuzzy analytic hierarchy process within a capital investment study**, *Journal of Economics and Management*, 1.2: pp. 207–230, 2005.

25.Wei, Guiwu, et al. **A linear assignment method for multiple criteria decision analysis with hesitant fuzzy sets based on fuzzy measure**, *International Journal of Fuzzy Systems*, 19.3: pp. 607–614, 2017.

26.Suder, Asli; Kahraman, Cengiz,**Multicriteria analysis of technological innovation investments using fuzzy sets**, *Technological and Economic Development of Economy*, 22.2: pp. 235–253, 2016.

27.M.G. Abdel-Kader, D. Dugdale, P. Taylor, ***Investment decisions in advanced manufacturing technology: A fuzzy set theory approach***, Routledge, 2018.

28. M.L. Priyanka, S.Rajeshwari, K.Ashwini,**An Expert model for DNA Based Encryption Technology using Cloud Computing,***International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE)*, Vol. 8, No.1.3, pp.15-18, 2019. https://doi.org/10.30534/ijatcse/2019/0381.32019

29. B.Akhmetov, V.Lakhno, Y.Tkach, A.Adranova, G.Zhilkishbayeva,**Problems of Development of a Cloud-Oriented Educational Environment of the University,** *International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE)*, Vol. 9, No.2, pp.2196-2203, 2020. https://doi.org/10.30534/ijatcse/2020/196922020

30. B. Madhuravani, N.Chandra Sekhar Reddy, K.Sai Prasad, B.Dhanalaxmi, V. Uma Maheswari,**Strong and Secure Mechanism for Data Storage in Cloud Environment,***International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE)*, Vol. 8, No.1.3, pp.29-33, 2019. https://doi.org/10.30534/ijatcse/2019/0681.32019