A Model for Managing the Procedure of Continuous Mutual Financial Investment in Cybersecurity for the Case with Fuzzy Information

Berik Akhmetov, Valeriy Lakhno, Volodimir Malyukov, Bakhytzhan Akhmetov, Bagdat Yagaliyeva, Miroslav Lakhno, and Yakiyayeva Gulmira

Abstract The paper looks at the development of a mathematical model of the process of continuous mutual investment of projects in the sphere of information security and information protection within the framework of a scheme with fuzzy information. The proposed model is the core of an intelligent support system of accepting decisions in the analysis of different investment plans of information security systems for information objects of informatization, particularly national centers for responding to cyber threats from investors from different countries. The model makes it possible to use the toolkit of a quality game surfaces in the case when the information support of investors is specified by means of fuzzy sets. Particularly, this information support may relate to fuzzy data on the size of investors' financial resources or technologies used to protect information and the corresponding risks of their implementation. The paper presents the outcomes of experiments accomplished in the MATLAB modeling simulation environment. The online platform of the support system of making decisions of investors is also described when choosing an investment plan of information protection systems of an informatization object. The outcomes of simulation have confirmed the performance and capability of the model for the analysis of different strategy investment in information protection systems of an informatization object, taking into account fuzzy information.

B. Akhmetov · B. Yagaliyeva (✉)
Yessenov University, Aktau, Kazakhstan
e-mail: bagdat.yagaliyeva@yu.edu.kz

B. Akhmetov
e-mail: berik.akhmetov@yu.edu.kz

V. Lakhno · V. Malyukov · M. Lakhno
National University of Life and Environmental Sciences of Ukraine, Kiev, Ukraine

B. Akhmetov
Kazakh National Pedagogical University, Almaty, Kazakhstan

Y. Gulmira
Khoja Akhmet Yassawi Kazakh-Turkish International University, Turkistan, Kazakhstan
e-mail: gulmira.yakiyaeva@ayu.edu.kz

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

P. Karrupusamy et al. (eds.), *Sustainable Communication Networks and Application*,
Lecture Notes on Data Engineering and Communications Technologies 93,
https://doi.org/10.1007/978-981-16-6605-6_40

Keywords Information security · Information security systems · Investment · Optimal strategies · Differential game · Decision support system · Fuzzy sets

1 Introduction

The quick development of information technology (IT) made it necessary to pay due attention to ensuring information security (IS) of various objects of informatization (OIN). This solves the problem of ensuring compliance of the state of a specific IT with rapid changes in the landscape of information threats for OIN. This, in turn, reduces the likelihood of risks associated with information threats. In the formation of information security systems (ISS) in many companies, enterprises, and institutions, the greatest attention is paid, as a rule, to the fulfillment of the requirements of the regulatory and methodological framework in the field of information security (IS), defining these requirements as the fundamental basis for the formation of ISS. However, without a suitable degree of investment in the ISS of OIN, these activities, by themselves, do not yet create guarantees of a sufficient level of IP. Nevertheless, the question of the ratio of the costs of building an information security system (ISS) and possible losses from the implementation of information threats in the absence or insufficient reliability is still poorly studied. Taking this into account, the question of determining the amount of investment, that is advisable to invest in the information protection of OIN, should be recognized as still relevant.

An organization can allocate significant resources to ensure the stability and stability of the functioning of corporate information systems, but this does not guarantee the achievement even of the minimum level of security of information resources. The essence of the problem is that in the design and construction of information security systems, the main attention should be paid not to minimizing the impact of a certain list of typical information threats (which is often compiled for a certain imaginary environment for the OIN functioning) but to the search for optimal investment management strategies, including mutual strategies for different ratios of criteria of the investment procedure in the OIN in the context of fuzzy information about investors.

The provision of IS of OIN is possible only through the comprehensive and continuous application of organizational, legal, and technical protection methods at different levels of implementation. In order to develop common approaches in countering cyber threats, to consolidate efforts in the investigation and prevention of cybercrimes, to prevent the use of cyberspace for illegal and military purposes, many leading states [1, 2] have stepped up their participation in organizing joint international projects to build cyber potential, which in fact are examples mutual investment in the OIN.

In this context, Ukraine and Kazakhstan continue to apply European and international standards in the field of cybersecurity, develop the work of relevant bodies that are able to effectively interact with the relevant bodies of the EU and NATO. The experience of Ukraine and Kazakhstan allows them to be not only recipients of

assistance from the EU and NATO states but also sources of new knowledge, skills and ways to counter modern cyber threats.

Many experts in the field of cybersecurity have noted that the use of intelligent information systems, which certainly include decision support systems or expert systems for finding the optimal strategy for investing in cybersecurity circuits, can be useful. This primarily concerns multilateral interstate projects. That is, such projects in which the optimal solution should take into account the balance of interests of many players in the investment market of information security systems and cybersecurity. An expert person, no matter how qualified he is, is unable to cover dozens of interrelated factors that can affect the success of investing in such a complex area as information security and cybersecurity [3, 4].

In its turn, the increasing complexity of the architecture of an intelligent system entails the need to apply more complex algorithms and corresponding mathematical models. In such problems, it is impossible to do with simple linear dependencies, which were used 10–15 years ago. Today, it is not enough just to calculate the payback period of investments in information security and cybersecurity projects. It is crucial to take into account dozens of external factors, and most importantly, to realize clearly that the procedure for investing in information protection and cybersecurity circuits takes place in conditions of constant confrontation with the attacker. Moreover, the attacking party of the defense is not bound by any ethical or legislative norms and is aimed at achieving his goals at any cost.

2 Literature Review and Problem

The economic efficiency of the information security system is an important and often a determining indicator of the effectiveness of such systems [3, 4]. A description of the investment model in information security systems and probabilistic models of losses from attacks are proposed in the work [5]. These models allow describing the mathematical expectation and variance of losses for the information security system in an analytical form. On this basis, a methodology has been developed for assessing the effectiveness of investments and economic risk for ISS [3, 4]. As a generalized indicator of investment efficiency, it is proposed to use the degree of risk for a random variable (R.V) of the net present value (NPV) of total costs for the ISS. This measure of risk is equal to the sum of the mathematical expectation of R.V. cost and its standard deviation multiplied by the coefficient k, but it is noted that a necessary condition for the adequate application of stochastic models is the mandatory availability of reliable statistical and expert data on attacks and security measures [4, 5]. And this is not always possible. Therefore, naturally, in relation to the models considered in [3, 5], the question arises about the influence of input data errors on the resulting indicators.

The model proposed in [6] uses optimization methods to analyze the investment levels in cybersecurity measures and insurance for owners of critical infrastructure

facilities. This model can be used to develop strategies to minimize cybersecurity risks. However, the authors do not provide a software solution.

In recent years, many researchers have increased interest in the scientific substantiation of the solution to the problem of defining optimal methods for investing in information security systems. Particularly, such fundamental research can be mentioned in [4, 7].

It is shown in [8] that it is possible to achieve a given level of IS of the OIN only by comprehensively solving financial, design, production, organizational, research and other interrelated tasks. Consistency has undoubtedly become an advantage of this approach. However, in the work, the authors did not provide an assessment of the potential for using the DSS in such complex tasks to assure the information security of the OIN.

The model proposed in [3, 4, 9] (hereinafter referred to as the GL model) has become one of the most popular for practical assessment of investment strategies in the IS of the OIN. However, this model, and its numerous modifications [10, 11], do not take into account the real mechanisms of return on investment to investors. This led to the limitations of the practical aspects of the application of this model.

The development of intelligent computing [12] gave a powerful impetus to such an independent direction of applied research as the development of intelligent DSS in the process of choosing optimal strategies for investing in ISS. It should be noted that the results of this research, and particular works [12–14], showed that often the proposed ones do not allow generating real recommendations for investors in the information security system. This is especially manifested in situations where there is no clear information about the aspects of investment, for example, the maximum amount of resources allocated for investment projects to create information security information objects of informatization. As the authors admit in [14, 15], the proposed models lack the properties of adaptability. That is, it is necessary to make adjustments to them even with a slight change in the initial parameters and boundary conditions in the process of analyzing investment strategies in projects related to IS and ISS.

In [16, 17], the authors showed that investing in information security should be considered comprehensively from the point of view of various tasks arising in the course of providing information security for the OIN. Investment areas include: anti-virus software (software), firewalls, cryptographic systems, intrusion detection systems; automated backup systems, etc.

The aforementioned necessitated the development of new adaptive models for the DSS [18] in terms of determining optimal strategies for mutual financial investment in ISS projects.

As shown in [19], hackers are often more motivated to achieve their goals, while the defense side is often satisfied only with the return on investment in the information security system. While the defense side can spend huge sums of money on the cybersecurity of OIN, hackers may have to invest only a small portion of their financial resources in the attack, for example, by bribing an unscrupulous employee who is willing to “help” to overcome OIN security perimeters.

Taking into consideration the results presented in [20, 21], it can be stated that the use of intelligent information systems can give a new impetus to seek for solutions in

the problems of optimizing investment strategies in information security and cybersecurity systems of complex multi-circuit distributed information systems. Moreover, nowadays such distributed systems often form the basis of the business processes of many companies and organizations around the world. Consequently, the search for mathematical models of the computing core for such intelligent systems is still relevant. And the game theory acts, namely its subsection concerning the description of the quality games procedure as a variant of the solution that has confirmed its functionality.

3 Purpose and Objectives of the Research

The purpose of the work is to develop a model for the module of a computer support system of decision making in the course of discrete mutual investment in ISS on condition of fuzzy information about investors. To achieve the goal, the following tasks are solved:

- the optimal strategies of investors have been determined for a situation when there is unclear information from the defense party;
- simulation modeling is performed in the MATLAB environment using the developed online DSS platform for various strategies for investing in information security systems in a fuzzy formulation.

4 Models and Methods

The landscape and scale of cyberattacks force the OIN defense side to prioritize defensive methods and techniques. This means that an organization or an enterprise must take into account the full range of information security threats to which they are exposed. The risks of losing information resources as a result of an attack must also be considered, and actions must be taken to minimize the vulnerabilities that are identified. All of the above tasks are quite difficult. In doing so, bear in mind that: (1) often information security administrators and ISU management do not always have a clear budget for ISS; (2) do not have clear information on the ratio of cost of attack/size of losses; (3) the pans for financing the information security system in the short term is not always defined.

Despite the fact that investments in information security are constantly being given great attention by practitioners and the academic community, the number of cyber incidents, violations of the information security perimeter, and unauthorized intrusions into information systems is steadily increasing.

In most cases, this is due to a lack of understanding of investment strategies in the information security of OIN. And this, in turn, leads to the adoption of erroneous decisions. Such solutions will not be viable in terms of cost/benefit ratio. This is due to the fact that attempts to correct potential vulnerabilities of OIN information

systems in "manual mode" in order to avoid information security violations often leads to excessive investments in information security systems.

Let us consider this situation. An investor (player 1 or *RG1*) in the field of information security (IS) from a state where a stronger currency (*VL1*) is used in monetary circulation, having free financial resources (hereinafter *FRE*), strives to accept the most desirable options for its placement in information protection technology, for example, for a national cyber monitoring center in another country. To do this, he must choose a counterparty (player 2 or *RG2*). The counterparty uses a weaker currency by default $-VL2$. This situation is typical, for example, when investing in projects to create national information security centers in developing countries.

Investors need to assess the priority of investing their financial resources in such areas of development and relevant technologies that provide IS of OIN (for example, an information security situation center or a monitoring center) as: (1) ensuring the cybernetic stability of OIN; (2) innovative technologies in the tasks of monitoring the risk indicators of the implementation of information threats and ensuring the required level of information security; (3) culture of information security at OIN; (4) information security of the network infrastructure; (5) security of software (software); (6) security of data processing technologies; (7) and others.

The problem of studying strategies for investing in the ISS of OIN can have many different, nonequivalent mathematical formulations. Depending on the setting of the task and the mathematical apparatus used for their analysis, various approaches can be used. This proves the importance of a flexible approach to the mathematical formulation of the problem.

Based on the analysis of the attractiveness of investment strategies for different investors representing different states, as indicated above, the mathematical apparatus of game theory was used.

Conceptually, the interaction of players (hereinafter denoted as $RG1$ and $RG2$) will be described this way: $RG1$, having some free financial resources (*FRE*), increases them at time *g1* (g1 is the rate of growth of resources *RG1).* Further, for example, using the DSS, it is decided what part of these resources will be directed to active operations to create a national center for monitoring information security and cyber threats. These operations involve the allocation of resources $RG1$ in investment projects as a part of building an information security system for OIN. The part of the resource is used to pay off the debt that exists at *RG1* in this period of time. We believe that it does the same with respect to *RG2*. In the proposed model, the following assumptions are made:

(a) $RG1$ FiR h valued at $VL1$ (currency 1);
(b) $RG2$ controls the FIR of q valued at $VL2$ (currency 2);
(c) throughout the interaction, the ratio of $VL1$ to $VL2$ (the exchange rate) k_d remains constant; player $RG1$ has no idea of the financial resources of $RG2$. He has only information that they belong to the fuzzy set $\{X, m(.)\}$. Here X is a subset $R_+ m(.)-$ function of the second investor's FiR $q(0)$ value belonging to the set $X, m(q(0)) \in [0, 1]$ for $q(0) \in X$. In addition, at each moment t $(t \in [0, T])$ his states are known $h(\tau)$ for $\tau \leq t$. The following conditions

are satisfied: $h(\tau) > 0$ when condition $h(\tau) \succ 0$ is satisfied with reliability $\geq p_0 (0 \leq p_0 \leq 1)$ and $h(\tau) \prec 0$ when condition $h(\tau) \prec 0$ is satisfied with reliability $\prec p_0$, and the values of realizations of strategy $u(\tau)(\tau \leq t)$, allocated for interaction with $RG2$ are also known.

4.1 A Model Describing Player Interactions

Further in the text of the paper, we will assume, respectively, that the players are designated as RG1 and RG2. The players have their own resources, which they are ready to invest either permanently or for a certain period of time in the information security or cybersecurity systems of the company. Players can have active operations. For example, at certain moments of investment, resources must be directed to active operations. As an example of such an active operation from the point of view of the classical approach of the interacting parties of the investment process, one can point to the mutual repayment of debts that accumulate among the parties during the implementation of information protection projects. The interactions between players and their resources are described by the following system of equations:

$$\begin{aligned} dh(t)/dt = & -h^+(t) + g_1 \cdot h^+(t) \\ & + [(1 - f_1(t)) \cdot (m_1(t) + p_1(t)) - 1] \cdot u(t) \cdot g_1(t) \cdot h^+(t) \\ & + [1 - (m_2(t) + p_2(t)) \cdot (1 - f_2(t))] \cdot v(t) \cdot g_2(t) \cdot \frac{q^+(t)}{k_d}; \end{aligned} \quad (1)$$

$$\begin{aligned} dq(t)/dt = & -q^+(t) + g_2 \cdot q^+(t) \\ & + [(1 - f_2(t)) \cdot (m_2(t) + p_2(t)) - 1] \cdot v(t)(t) \cdot q^+(t) \\ & + [1 - (m_1(t) + p_1(t)) \cdot (1 - f_1(t))] \cdot u(t) \cdot g_1(t) \cdot h^+(t) \cdot k_d. \end{aligned} \quad (2)$$

and

$$h^+ = \left\{ \begin{matrix} h, h \geq 0 \\ 0, h \prec 0 \end{matrix} \right\}., q^+ = \left\{ \begin{matrix} q, q \geq 0 \\ 0, q \prec 0 \end{matrix} \right\}.$$

Thus, at time t, the value of $dh(t)/dtRG1$ (in $VL1$) is equal to:

$g_1(t) \cdot h^+(t)$, the amount of interest $m_1(t) \cdot (1 - f_1(t)) \cdot u(t) \cdot g_1(t) \cdot h^+(t)$ for the invested FiR $RG1$;

$(1 - f_1(t)) \cdot u(t) \cdot g_1(t) \cdot h^+(t)$—the size of the invested FiR of $RG1$;

$p_1(t) \cdot (1 - f_1(t)) \cdot u(t) \cdot g_1(t) \cdot h^+(t)$—the value, which characterizes the share of the "returned" investment resource (hereinafter InR) $RG1$;

$(1 - f_1(t)) \cdot u(t) \cdot g_1(t) \cdot h^+(t)$—R $RG1$ for ISS;

$\left[\{(1 - p_2(t)) \cdot (1 - (f_2(t)/k_d))\} \cdot v(t) \cdot g_2(t) \cdot q^+(t)\right]$—the value of the "unrecovered" asset (investment) $RG2$ (in $VL1$);

$\left[\{f_2(t)/k_d\} \cdot v(t) \cdot g_2(t) \cdot q^+(t)\right]$—resources to repay the debt $RG2$ to $RG1$.;

$u(t) \cdot f_1(t) \cdot g_1(t) \cdot h^+(t)$—the resource allocated to pay off the debts incurred by $RG1$ at time t to $RG2$;

$u(t) \cdot (1 - f_1(t)) \cdot g_1(t) \cdot h^+(t)$—the resource allocated to carry out the investment in ISS OIN at time t;

$\{g_2(t) \cdot (1 - (f_2(t)/k_d))\} \cdot v(t) \cdot g_2(t) \cdot q^+(t)$—interest charge for the InR $of\, RG2$;

$\{(1 - (f_2(t)/k_d))\} \cdot v(t) \cdot g_2(t) \cdot q^+(t)$—InR $of\, RG2$.

$h^+(t)$ is the value subtracted from this sum.

Similar terms will be for expression (2). Thus, the value of $dq(t)/dt$ (in $VL2$) at time t is equal to the sum of such terms:

$g_2(t) \cdot q^+(t)$, values of interest $m_2(t) \cdot (1 - f_2(t)) \cdot v(t) \cdot g_2(t) \cdot q^+(t)$ for invested FiR $RG2$;

$(1 - f_2(t)) \cdot v(t) \cdot g_2(t) \cdot q^+(t)$—the size of InR $of\, RG2$;

$p_2(t) \cdot (1 - f_2(t)) \cdot v(t) \cdot g_2(t) \cdot q^+(t)$—the value characterizing the share of the "returned" InR $RG1$ to $RG2$;

$(1 - f_2(t)) \cdot v(t) \cdot g_2(t) \cdot q^+(t)$—InR $RG2$ on ISS;

$(1 - p_1(t)) \cdot (1 - f_1(t)) \cdot u(t) \cdot k_d(t) \cdot g_1(t) \cdot h^+(t)$—is the value of the "unreturned" asset (investment) in $RG1$ by player $RG2$;

$u(t) \cdot f_1(t) \cdot k_d(t) \cdot g_1(t) \cdot h^+(t)$—is the value characterizing the repayment of $RG1$ debt to $RG2$;

$v(t) \cdot f_2(t) \cdot g_2(t) \cdot q^+(t)$—is the amount allocated to $RG2$ to repay the debt it has owed to $RG1$ at time t;

$(1 - f_2(t)) \cdot v(t) \cdot g_2(t) \cdot q^+(t)$—the value allocated by $RG2$ to make investments in ISS at time t;

$m_1(t) \cdot (1 - f_1(t)) \cdot k_d(t) \cdot u(t) \cdot g_1(t) \cdot h^+(t)$—is the percentage charge for the InR $RG1$;

$(1 - f_1(t)) \cdot u(t) \cdot g_1(t) \cdot h^+(t)$—InR $of\, RG1$.

The value of $q^+(t)$ is subtracted from this amount;

The interaction ends when the conditions are met:

$$(h(t), q(t)) \in S_0 = \big\{\big((h(t),\ q(t) \in S_0^*, \text{with reliability} \geq p_0, (h(t), q(t)) \in S_1^*, \text{with reliability} \geq p_0\big\} \tag{3}$$

$$(h(t), q(t)) \in F_0 = \big\{\big(((h(t),\ q(t)) \in S_0^*, \text{with reliability} \prec p_0, (h(t), q(t)) \in S_1^*, \text{with reliability} \prec p_0\big\} \tag{4}$$

where

$$S_0^* = \big\{(h, q) : (h, q) \in R_+^2, h > 0\big\},$$
$$S_1^* = \big\{(h, q) : (h, q) \in R_+^2, q = 0\big\},$$

If it turns out that condition (Eq 3) is fulfilled, then we will say that in the process of investing in the ISS of OIN has achieved the desired result with confidence $p \geq p_0$ and the procedure is completed.

If it turns out that the condition (Eq 4) is fulfilled, then we will say that in the procedure of investing in the SPI, the SPI has achieved the desired result with confidence $p \succ 1 - p_0$ and the process is completed.

If both condition (Eq 3) and condition (Eq 4) are not carried out, then the process of investing in ISS of OIN continues further.

Define the function $F(.) : X \to R_+$, $F(x) = \{\sup m(y) \text{ for } y \leq x\}$.

Denote by Φ the set of such functions, by $T^* = [0, T]$,—the time segment.

Strategy of $RG1$ is the rule that allows him to determine the amount of FiR based on the available information, that $RG1$ allocates to invest in ISS of OIN.

The second player $RG2$ chooses his plan $v(.)$ on the base of any information that is available.

The first player *RG1* tries to figure out the set of his initial states. The set of such states and the preference set of the first player W_1 are presented [21]. Then, the plans of the first player will be called as his optimal plans. The goal of the first player is $RG1$ to find the preference set and to find his strategies. Applying them he will obtain the fulfillment of condition (3).

The formulated game model corresponds to the classification of the decision making theory and the problem of decision making in terms of fuzzy information. In order to describe the preference sets *of* $RG1$ it is crucial to include the value:

$$\phi(0) = \inf\{\phi'\},$$
$$F(\phi') \geq p_0.$$

Further, the solutions are made, i.e., "preference" sets Z_1 and optimal strategies $u_*(.)$ with all game parameter ratios. It is the set of such initial states $(h(0), \phi(0))$.I If the game starts from them, there exists a plan of $RG1$, which, for any realizations of plan $RG2$, "leads" at time t of the system state $(h(0), \phi(0))$ in which condition (3) will be accomplished. In that case, $RG2$ is lack of the strategy that can "lead" to the fulfillment of condition (4), at one of the previous times.

The paper touches on the following issue. How to determine the time of possible loss of capitals (i.e., INR) with a given degree of confidence using information about the initial FiR(capitals), the exchange rate, the growth rate of resources of *RG1* and *RG2*, percentage rates on allocated capitals, levels of payable and receivable debts, fuzzy information on FiR of the second player related to the use of new information security technologies, and cybersecurity?

We have used the apparatus of the theory of multistep quality games as a toolkit to find out the problem [21, 22]. This method allows determining the areas of possible initial states of resources (capitals) of parties. Therefore, we assume that the objects have the following property: if the interaction begins from these states, then the loss of capital is possible at time t either by one side of the party or by the other, and it gives the answer to the given question. A multistep quality game with two quality surfaces

has been defined in order to find such areas. The solution involves the determination of the preferences of the parties. Furthermore, the optimal strategies of the parties have been revealed while investing in the OIN information security system (using the example of an international situational center on information security).

Within the framework of the research, we have made an attempt to consider a plain option for interaction allowing us to draw qualitative conclusions about the financial condition of the subjects. And it can also be quite easily applied algorithmically in any high-level programming language.

4.2 The Solution of the Problem

The solution of the problem consists of finding the preference set and its optimal strategies (the problem from the first ally player's point of view [21, 23]). Similarly, the problem is set from the point of view of the second ally player. Due to the symmetry of the problem statement, it is sufficient to solve the problem from the viewpoint of the first allied player. Solving the problem from the second allied player's point of view is similar.

The solution to **Problem 1** is found using the toolkit of the theory of multistage games with complete information [24], which allows finding the solution to the game for various ratios of the game parameters. Let us give the solution to the game, i.e., sets of preferences and optimal strategies $RG1$.

Suppose that the conditions are carried out at any time t:

$$g_1(t) = g_1; \quad g_2(t) = g_2;$$
$$f_1(t) = f_1; \quad f_2(t) = f_2; \quad p_1(t) = p_1; \quad p_2(t) = p_2.$$

Denote through z_1 & z_2 the following quantities:

$$z_1 = (1 - f_1) \cdot (m_1 + p_1) - 1, z_2 = (1 - f_2) \cdot (m_2 + p_2) - 1.$$

There are four possible cases:

$$a) \quad z_1 \geq 0; \quad z_2 \geq 0; \quad b) \quad z_1 \prec 0; \quad z_2 \prec 0;$$
$$c) \quad z_1 \succ 0; \quad z_2 \leq 0; \quad d) \quad z_1 \leq 0; \quad z_2 \succ 0.$$

Let us give the solution to the game, i.e., a set of preferences W_1 and optimal strategies of the first player.

For the case a) we have:

$$W_1 = \left\{(h(0), \phi(0)) : (h, \phi) \in \text{int } R_+^2, \ \phi(0) \prec w^* \cdot h(0)\right\} \tag{5}$$

for

$$w^* = \left\{ \frac{-[z_2 \cdot g_2 + g_2 - z_1 \cdot g_1 - g_1]/[2z_2 \cdot g_2] +}{\sqrt[2]{\{[z_2 \cdot g_2 + g_2 - z_1 \cdot g_1 - g_1]/2z_2 \cdot g_2\}^2 + (z_1 \cdot g_1)/(z_2 \cdot g_2)}} \right\}; \quad (6)$$

$u_*(h, \phi) = \{1,\ \phi < w \cdot h,\ (h, \phi) \in \text{int}R_+^2\}$ is not defined, else}.
In case (b) and (c) the quantity of W_1 is empty.
In case (c) and $g_2 > g_1 + z_1 \cdot g_1$ we get

$$W_1 = \{(h(0), \phi(0)) : (h(0), \phi(0)) \in \text{int}R_+^2,\ \phi(0) < \delta \cdot h(0)\}. \quad (7)$$

For $\delta = (z_1 \cdot g_1)/(g_2 - z_1 \cdot g_1 - g_1)$; $u_*(h, \phi) = \{1, \phi < \delta \cdot h,\ (h, \phi) \in \text{int}R_+^2\}$, is not defined, else
In case c) and $g_2 \le g_1 + z_1 \cdot g_1$ we have:

$$W_1 = \text{int}R_+^2,\ u_*(h, \phi) = \{1, (h, \phi) \in \text{int}R_+^2\}, \quad (8)$$

is not defined, else.
Problem 2 is defined symmetrically (from the second ally player's standpoint).

5 Imitation (Simulation) Experiment

In order to illustrate the results of the calculation, they are carried out for the data that are adopted for the information protection and cybersecurity systems of the situation center of the Ministry of Transport of Kazakhstan. This center is a vivid example of investment interaction in the field of information protection and cybersecurity of many states, including Kazakhstan, China, countries of the European Union, etc. Simulation modeling is performed in the MATLAB package. Some of the outcomes obtained during the simulation are illustrated in Figs. 1 and 2.

In the graphs Figs. 1 and 2, h-axis means "million" $ (in our case *VL1*). In Fig. 1, the tangent of the angle is equal to "2." In Fig. 2, the tangent of the angle is "3." Axis ϕ means million in local currency (e.g., Kazakhstan tenge or Ukraine hryvnia). In Figs. 1 and 2, the trajectories of investors are illustrated. In Fig. 1, the trajectory is in the preference area of the second investor and shown by a green dashed line with round green markers (line number 1). In Fig. 2, the trajectory of investors follows the ray of balance, which is the boundary of the preference area of the first investor, shown by a blue dotted line with markers in the form of rhombuses (line number 1). The balance beams are shown in Figs. 1 and 2 in red solid line with red round markers.

Figure 3 describes an example of the implementation of the proposed model on the online DSS platform.

Figure 3a shows an example of a solution describing the ratio of players' resources for a situation in which the trajectory (shown by the yellow line) of the first investor's movement is located in his area of preference.

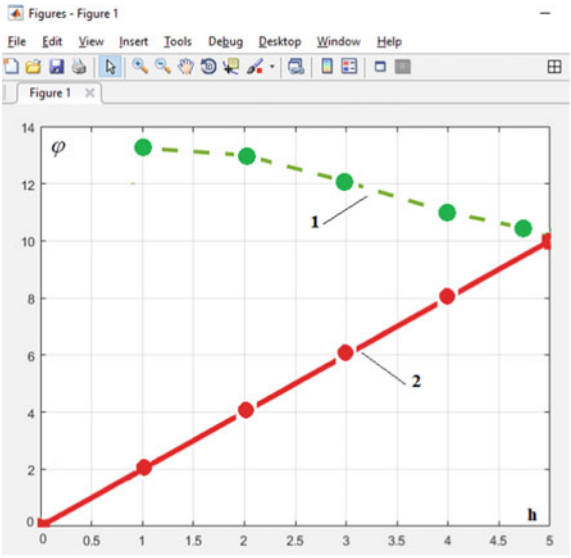

Fig. 1 Computational experiment No.1

1- Player trajectory; 2- Beam of balance

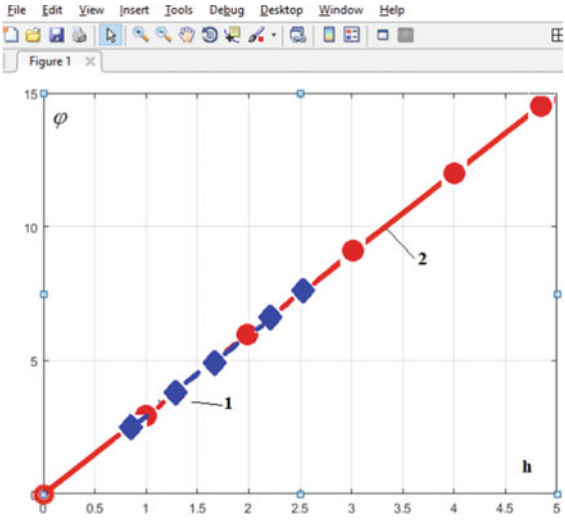

Fig. 2 Computational experiment No.2

1- Trajectory of the player's movement; 2- Beam of balance

Figure 3b shows histograms of step-by-step changes in the size of the FiR of the players for the first investor in red for the second in green.

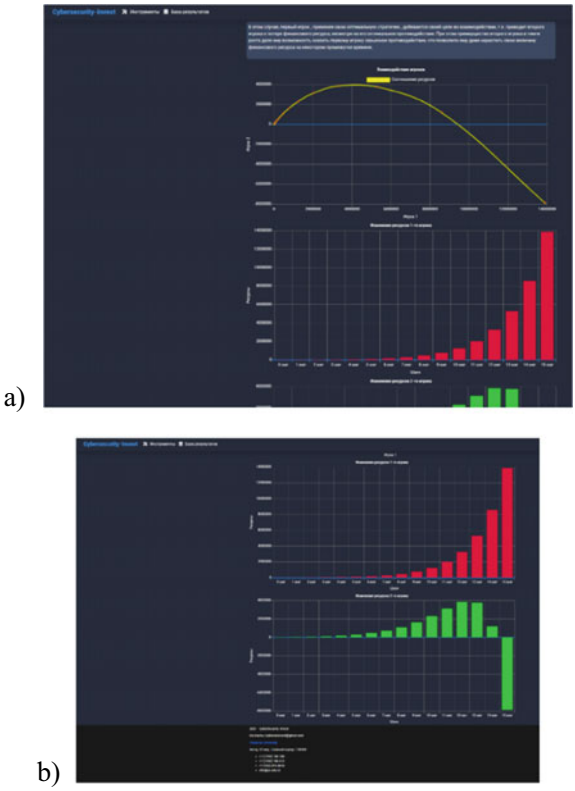

Fig. 3 General view of the DSS

6 Discussion

Thus, a new model is presented that describes the investment process in information security and cybersecurity systems of an informatization object. The model is based on the apparatus of game theory. The graphs in Figs. 1 and 2 are the results demonstrating the effectiveness and functionality of the game model. The graphs in Fig. 1 correspond to simulation experiment number 1. For this experiment, a result was obtained that would be typical for situations when RG2 player used the non-optimal behavior of RG1 at the initial time. If the trajectory moves under the balance beam (red line), then on the contrary, RG1 used the non-optimal behavior of RG2. Such a graph is not shown in the paper. But a situation is possible when the actions of the players and their investment strategies satisfy both parties. It will be a balanced investment strategy for both parties. In the case of a balanced strategy, both players and their investment trajectories will coincide with the balance beam.

To confirm the functionality of the proposed model, the obtained results were compared with other approaches that various authors proposed [6, 8–10, 25]. The outcomes achieved by us were close enough. However, the complexity of calculations

is less in accordance with our model. It has taken 11–14% of less time to obtain data than, for example, the models described in the works [8–10].

7 Conclusions

As part of the study, the following tasks have been solved:

A model of the process of continuous mutual investment of projects in the sphere of information security and information protection within the framework of a scheme with fuzzy information has been developed. The model has served as the core of the computing module of the intelligent support system in the analysis of various investment strategies in information protection systems of information objects. The model is based on the application of the tools of a quality game surfaces in case when the information support of investors is given by means of fuzzy sets;

Simulation experiments have been carried out in the MATLAB simulation environment;

The online platform of the decision making support system for investors is described while choosing a strategy of investing in ISS of OIN.

Acknowledgements This research was funded by Committee of Science MES RK, grant number AP08855887—«Development of intelligent decision support system in the process of investing in cybernetic security systems».

References

1. H.S. Lallie, L.A. Shepherd, J.R. Nurse, A. Erola, G. Epiphaniou, C. Maple, X. Bellekens, Cyber security in the age of covid-19: a timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Comput. Secur. **105**, 102248 (2021)
2. M.K. Kagita, N. Thilakarathne, T.R. Gadekallu, P.K.R. Maddikunta, S. Singh, A Review on cyber crimes on the Internet of Things, (2020). arXiv preprint arXiv:2009.05708
3. L. Gordon, M. Loeb, W. Lucyshyn, Information security expenditures and real options: a wait-and-see approach, Comput. Secur. J. **19**(2), 1–7 (2003)
4. L.A. Gordon, M.P. Loeb, L. Zhou, Information Segmentation and Investing in cybersecurity. J. Inf. Secur. **12**(1), 115–136 (2020)
5. D. Kosutic, F. Pigni, Cybersecurity: investing for competitive outcomes. J. Bus. Strategy. ahead-of-print(ahead-of-print), (2020). https://doi.org/10.1108/JBS-06-2020-0116
6. D. Young, J. Lopez Jr., M. Rice, B. Ramsey, R. McTasney, A framework for incorporating insurance in critical infrastructure cyber risk strategies. Int. J. Crit. Infrastruct. Prot. **14**, 43–57 (2016)
7. A. Yang, Y.J. Kwon, S.-Y.T. Lee, The impact of information sharing legislation on cybersecurity industry. Ind. Manag. Data Syst. **120**(9), 1777–1794 (2020). https://doi.org/10.1108/IMDS-10-2019-0536
8. L.A. Filimonova, N.K. Skvortsova, On issue of algorithm forming for assessing investment attractiveness of region through its technospheric security, in *IOP Conference Series: Materials Science and Engineering—IOP Publishing*, vol. 262, no. 1, p. 012196, (2017). https://doi.org/10.1088/1757-899X/262/1/012196

9. L.A. Gordon et al., The impact of the Sarbanes-Oxley Act on the corporate disclosures of information security activities. J. Account. Public Policy **25**(5), 503–530 (2006). https://doi.org/10.1016/j.jaccpubpol.2006.07.005
10. W. Qin, Z.H.U. Jianming, Research on the game of information security investment based on the Gordon-Loeb model. J. Commun. **39**(2), 174 (2018). https://doi.org/10.11959/j.issn.1000-436x.2018027
11. X. Li, Decision making of optimal investment in information security for complementary enterprises based on game theory. Technol. Anal. Strategic Manage.1–15 (2020). https://doi.org/10.1080/09537325.2020.1841158
12. Y. Li, L. Xu, Cybersecurity investments in a two-echelon supply chain with third-party risk propagation. Int. J. Prod. Res. **59**(4), 1216–1238 (2021)
13. M. Benaroch, Real options models for proactive uncertainty-reducing mitigations and applications in cybersecurity investment decision making. Inf. Syst. Res. **29**(2), 315–340 (2018)
14. K.K.F. Yuen, Towards a cybersecurity investment assessment method using primitive cognitive network process, in *2019 International Conference on Artificial Intelligence in Information and Communication (ICAIIC)* . IEEE, 2019), pp. 068–071
15. A. Fielder, E. Panaousis, P. Malacaria, C. Hankin, F. Smeraldi, Decision support approaches for cyber security investment. Decis. Support Syst. **86**, 13–23 (2016)
16. Y. Lee, R. Kauffman, R. Sougstad, Profit-maximizing firm investments in customer information security. Decis. Support Syst. **51**(4), 904–920 (2011)
17. B. Srinidhi, J. Yan, G.K. Tayi, Allocation of resources to cybersecurity: the effect of misalignment of interest between managers and investors. Decis. Support Syst. **75**, 49–62 (2015)
18. B. Akhmetov, V. Lakhno, B. Akhmetov, Z. Alimseitova, Development of sectoral intellectualized expert systems and decision making support systems in cybersecurity, in *Proceedings of the Computational Methods in Systems and Software* (Springer, Cham, 2018), pp. 162–171
19. L. Xu, Y. Li, J. Fu, Cybersecurity investment allocation for a multi-branch firm: modeling and optimization. Mathematics **7**(7), 587 (2019)
20. B.B. Akhmetov, V.A. Lakhno, B.S. Akhmetov, V.P. Malyukov, The choice of protection strategies during the bilinear quality game on cyber security financing. Bull. Nat. Acad. Sci. Repub. Kaz **3**, 6–14 (2018)
21. V. Lakhno, V. Malyukov, N. Gerasymchuk et al., Development of the decision making support system to control a procedure of financial investment. Eastern-Eur. J. Enterp. Technol. **6**(3), 24–41 (2017)
22. R. Casado-Vara, F. Prieto-Castrillo, J.M. Corchado, A game theory approach for cooperative control to improve data quality and false data detection in WSN. Int. J. Robust Nonlinear Control **28**(16), 5087–5102 (2018)
23. A. Agah, S.K. Das, K. Basu, A game theory based approach for security in wireless sensor networks, in *IEEE International Conference on Performance, Computing, and Communications*, (IEEE, 2004), pp. 259–263
24. B. Yang, C. Lai, X. Chen, X. Wu, Y. He, Surface water quality evaluation based on a game theory-based cloud model. Water **10**(4), 510 (2018)
25. L. Gordon, M. Loeb, W. Lucyshyn, L. Zhou, The impact of information sharing on cybersecurity underinvestment: a real options perspective. J. Account. Public Policy **34**(5), 509–519 (2015)