CONCEPTUAL DIAGRAM OF AN INTELLIGENT DECISION SUPPORT SYSTEM IN THE PROCESS OF INVESTING IN CYBERSECURITY SYSTEMS

[1]BERIK AKHMETOV, [2]VALERY LAKHNO, [3]BAGDAT YAGALIYEVA, [4]LAZAT KYDYRALINA, [5]NURZHAMAL OSHANOVA, [5]SALTANAT ADILZHANOVA

[1,3]Yessenov University, Kazakhstan
[2]National University of Life and Environmental Sciences of Ukraine, Department of Computer Systems and Networks, Ukraine
[4]NAO «Shakarim University in Semey», Kazakhstan
[5]Abai Kazakh National Pedagogical University, Kazakhstan
[6]Al-Farabi Kazakh National University
E-mail: [1]berik.akhmetov@yu.edu.kz, [2]lvaua21@gmail.com, [3]bagdat.yagaliyeva@yu.edu.kz

ABSTRACT

The article proposes a structural diagram of the functioning of a DSS in the process of analyzing and choosing a rational (optimal) strategy for investing in cybersecurity systems (CrS) in a dynamic confrontation with the opposing side (hacker). The key functional modules of such a DSS are considered, which contribute to ensuring its continuous and efficient operation. Detailed block diagrams are given for the following key subsystems of this DSS: analysis of the problem, risks and threats associated with insufficient investment in CrS of an informatization object (OBI); the formation of goals and criteria for evaluating the effectiveness of investment in CrS of an OBI; formation of decisions; formation of the decision rule and analysis of alternative strategies for investing in CrS of the OBI. The above scheme provides full-featured decision-making in the process of choosing rational strategies for investing in cybersecurity systems of objects of informatization of any scale, from small companies or enterprises to large OBI. The article describes the results of computational experiments obtained for the online DSS in the process of searching for a rational strategy for investing in CrS of an OBI.

Keywords: *Decision Support System, Investment, Cybersecurity, Object Of Informatization, Subsystem, Block Diagram Of The Algorithm*

1. INTRODUCTION

The constant complication of the decision-making process, in particular, managerial ones, together with the complexity of subject areas, which certainly include the tasks of ensuring cybersecurity (CrS) for various objects of informatization (OBI), as well as the interconnection of factors influencing decisions, necessitate the attraction of external funds to support decision making. Since we are talking mainly about solving problems for high organizational levels (for example, information systems of critical OBI), the "cost" of a wrong decision is currently too high and is constantly growing. If we talk about supporting decision-making in the tasks of investing in cyber security systems for various OBI, then the wrong choice of investment strategy, coupled with the rapid growth in the number and complexity of destructive influences from hackers on the IT infrastructure of public and private companies [1, 2], can lead not only to the loss of information arrays, reputation, but also to significant damage to the finances of the object of the cyber attack.

Protecting information is a complex and costly task. In addition to a sufficiently high level of investment in the cybersecurity system itself, at the same time it is necessary to solve the contradiction between the availability of information resources, and the required degree of their protection. As shown in [1-3], excessive protective measures can lead to a reduction in the usability of an organization's information resources. And in addition, they lead to the often-unwarranted benefit of overprotecting information.

Because of this, adequate presentation and processing of expert information in the decision-making process regarding the choice of a rational strategy for investing in CrS an OBI is a priority area of scientific research in many states, and pressing problems associated with these issues require new research in this area.

2. REVIEW AND ANALYSIS OF LITERATURE

A huge amount of information and data circulates in modern information systems, including documents containing state, commercial or official secrets, various personal data bases. Objects of informatization (OBI) should ensure an appropriate level of security of their own information resources, because unauthorized leakage, destruction or theft of at least some part of the data that is stored in them can lead to significant material (potential or real) losses, causing significant image damage or even human losses, as, for example, in the case of information leakage regarding state ciphers, government communications systems, operational plans for the movement of military equipment, and the like. Taking this into account, information resources and information and telecommunication systems of all levels that ensure the functioning of OBI must have an appropriate level of protection against unauthorized actions with information on the part of intruders. At the same time, the costs of building information protection and cybersecurity systems can exceed the amount of potential losses in the event of information leakage. The latter makes it necessary to develop algorithms for calculating the optimal and maximum amount of possible investments in the protection of information resources.

According to [7-10], only about 78% of organizations spend no more than 15% of their IT budget on activities related to information security, another 11% of organizations - from 16 to 20%, and only 7% of organizations - from 21 to 28%. Unfortunately, the overwhelming majority of recommendations on investment in cybersecurity are only empirical, based solely on the generalization of experience in the development and operation of existing information security and cybersecurity systems.

This is what explains the attention that attracted the article published in 2002 by American economists Lawrence A. Gordon and Martin P. Loeb [3], in which an attempt was made to theoretically and methodologically substantiate the maximum volume of investments in information security. The appearance of this article caused a wide resonance in scientific and professional circles, as evidenced by numerous reviews and comments of a different nature, in particular positive and critical remarks, constructive suggestions and additions [3, 4].

Without going into a detailed analysis of the positive and negative properties of the Gordon-Loeb model, we note that both the model itself and its numerous modifications are characterized by a significant drawback: a formally approximate way of constructing the model. For such an approach, the possibility of taking into account, when forming the structure and parameters of the model, information about the real capabilities of the opposing side (hackers) who also invest in the implementation of threats and attacks on the information resources of the attacked side is completely excluded. This leads to a significant limitation of the practical aspects of the application of this model and the objectivity of the conclusions obtained, including the main postulate about the value of the optimal investment in information protection.

After a series of large-scale cyberattacks on public and private companies, leaks of personal data of clients and employees [3,4], cybersecurity issues began to receive more and more attention. This issue was one of the top issues that attracted the attention of management and board of directors of companies around the world.

As the research results show [1, 5], today more than 2/3 of companies understand that in the future they cannot be limited by standard measures in the field of cybersecurity, and begin to implement modern solutions, including technologies of artificial intelligence, robotization, automation and analytics. Leaders in the field of investing in cybersecurity not only continue to increase the basic functionality of the information protection circuits of the OBI, but also revise approaches to the entire cybersecurity architecture. At the same time, less than 10% of respondents [5] believe that their information security services fully meet current needs. More than 75% of representatives of large companies and about 65% of representatives of small companies note that existing CrS tools solve only part of the tasks associated with protecting their business.

In the context of continuously increasing scenarios for conducting cyber attacks on information assets of state institutions, private companies and enterprises, their management inevitably raises the question of attracting additional investments to ensure the CrS of an OBI. In turn, solving issues related to optimizing the choice of an investment strategy in CrS requires the intellectualization of decision making, not least by using the potential of computer decision support systems (DSS) and expert systems (ES) [6, 7].

In the existing ES and DSS, the completeness and adequacy of the knowledge provided by the expert are limited due to the fact that the expert is a priori offered a certain specific scale for the introduction of his estimates. Therefore, there is an urgent need to develop a number of procedures that will allow more efficiently, correctly, without pressure on an expert, to receive, interpret, process, coordinate and aggregate individual expert assessments, taking into account these limitations. Also, the developed DSS should provide for the provision of experts with the opportunity to refine and adjust the previously entered own estimates, in the process of further use of the DSS. In fact, we are talking about the need to create a new type of DSS that could adapt to the level of competence of experts on a specific issue in the subject area - the choice of an investment strategy for the cybersecurity of an object of informatization [7-10].

A number of authors in their publications [7, 8, 11] believe that the development of such a direction of applied research as mathematical support for decision making in the course of choosing a rational investment strategy in complex infrastructure projects should be accompanied by a synthesis of new models and methods.

In the context of global computerization, according to [9, 10], new methods and models will form the computing core of intelligent DSS. This category of software products is already helping to simplify the task of finding rational strategies for investors.

Note that there are quite different approaches from the point of view of the mathematical apparatus used in such models. For example, the authors [10, 11] describe the use of classical economic and mathematical models. However, these models in most situations do not take into account many parameters of investment in complex infrastructure projects. In [12–14], the authors note that in relation to this class of problems, the most adequate approach in the process of finding a solution will be the application of game theory.

As the analysis of such studies has shown, most of the models and algorithms given in [13–17] do not contain real recommendations and predictive estimates for investors. DSS software offered on the market are not very suitable for the problem of real choice of strategies by investors. And their main drawback is the low information content of the graphical results obtained in the process of evaluating real investment projects and options for investors' actions.

This circumstance determines the necessity and relevance of the development of new models and software products focused on cross-platform use. The developed online platform of intelligent DSS will potentially be able to support decision support procedures in the search for rational strategies for continuous investment by a group of investors in complex infrastructure IT projects.

The lack of standardization of the information field and limited access to structured information regarding the degree of CrS of a particular OBI is one of the main problems in the field of information protection and cybersecurity in many states. As a result, today only a few government agencies, enterprises or private companies can say with confidence that they have full information about the state of affairs in the field of CrS of their informatization object. For most companies and organizations that do not have their own highly qualified cybersecurity personnel, or have insufficient resources to attract external CrS specialists and protect the information assets of their OBIs, the only option is to use the potential of DSS or ES to solve the problem of finding a rational strategy for investing in CrS. The need to solve the problem of intellectual support for decision-making on choosing a strategy for investing in CrS means motivation for developing a draft concept of a DSS in the field of CrS OBI (hereinafter - the Concept), including for critical computer systems (CCS).

The concept aims to identify ways and means of creating a DSS in the process of investing in cyber security systems, to provide users with reliable information about financial and other risks associated with the implementation of the chosen strategy for investing in cyber security systems.

The purpose of the study. Development of a concept and a basic functional diagram of a decision support system for choosing a rational investment strategy in cybersecurity systems of an informatization object.

3. METHODS AND MODELS

Let us formulate a general model for the computational core of the DSS.

There are two groups of players - investors in information protection (investor # 1, for example, the owner of an information resource). And the opposing side (investor # 2 (invests in organizing a cyberattack on OBI) is, for example, a hacker trying to overcome the OBI's protection and damage the information resources of the defensive side). Since the computing core is based on the theory of the game, the terminology of this branch of mathematics is further applied. Two groups of players (defense and attack) control a dynamic system in multidimensional spaces. Accordingly, the dynamical system (DS) is given by a set of bilinear differential equations with dependent motions. Many strategies and groups of players are defined for DS. Terminal surfaces are also defined for DS [12, 18]. The goal of the first group of players (defense of OBI) is to bring the DS with the help of their control strategies to their terminal surface, regardless of the actions of the second group of players (hackers). The goal of hackers is to bring DS with the help of their control strategies to their terminal surface, no matter how the defense side acts. The formulated problem statement generates several tasks in the search for a rational strategy for investing in OBI cybersecurity systems.

The decision support system in the process of investing in cyber security systems (hereinafter referred to as the DSS) is created for the purpose of its use by any interested persons in all institutions or enterprises for which the task of finding a rational investment strategy from the KB system in the face of an increase in the number and complexity of destructive impacts on information resources from computer intruders.

DSS is designed to solve the following tasks:

- creation of knowledge bases (KB) of data (DB) and a database for various situations related to the choice of a strategy for investing in CrS systems, development of software for maintaining a single electronic archive of strategies for investing in CrS OBI with differentiation of user access;

- creation of a single information space in the field of accounting for rational investment strategies in CrS systems, ensuring information interaction between DSS subsystems through internal standardization of data formats and exchange protocols;

- creation of a unified system for generating output documentation for choosing rational strategies for investing in CrS systems;

- maintaining a database of samples and templates of documents required by the decision-maker (DM);

- formation of analytical information for decision-making in graphic and printed form;

- ensuring the consistency, complexity and consistency of the development of informatization of investment in CrS systems using traditional forms and methods of support and control.

The main functions of a DSS for information and cyber security programs are usually regulated based on the need to comply with:

principles of complex analysis of CrS problems;

the possibility of combining formal and informal methods used in the decision support process;

principles of reliability and relevance of information related to the current state of the problem. At the same time, as a rule, they use all kinds of reports, statistical data, analytical reviews, as well as data received from monitoring subsystems;

principles of automated selection of methods and models for the intellectualization of decision support;

principles of further development of DSS states;

principles of dynamic management of the DSS in order to increase the efficiency of its functioning and the validity of the received recommendations and conclusions, which can be used by the decision-maker in the process of developing control actions;

the potential of the modules of analysis, operational management and control over the problem being solved.

To ensure the full functioning of the DSS, as a rule, it should include the following main modules and subsystems, see fig.1:

1. Database modules, knowledge base, bases of models and rules used for decision making.

2. Interface control system. Which is designed based on the DSS architecture - local or client-server.

3. Other modules and subsystems, the need for which is dictated by the specifics of the subject area.

DSS should provide the following types of decision support:

expert support;

automated solution output;

combined solution.

The core of the DSS (or ES) is the knowledge base (KB). This subject knowledge base will accumulate the knowledge of experts in the field of investing in cybersecurity projects. It is advisable to present knowledge in the format of heuristic rules.

Training and accumulation of new knowledge in the KB is as follows:

when considering a specific investment problem, a rule is formulated that ensures its solution;

developed rules, depending on the specifics of a specific task, are placed in the rule base.

The search for the required rule in the DSS rule base is implemented, for example, based on semantic models.

The block diagram of the functioning algorithm of the subsystem "Analysis of problems and risks for an investment project in the cybersecurity systems of an informatization object" is shown in Fig. 2.

There are four classes of the most common problems when investing in CrS of an OBI.

1. Standard problems. Problems of this class, as a rule, require the application of instructions set by the decision maker.

2. Well structured problems. Problems of this class have quantitative characteristics and indicators. To solve this class of problems, as a rule, they use economic and mathematical methods.

3. Poorly structured problems. Problems of this class have not only quantitative but also qualitative characteristics. To solve such problems, it is necessary to use the methods of system analysis in the DSS.

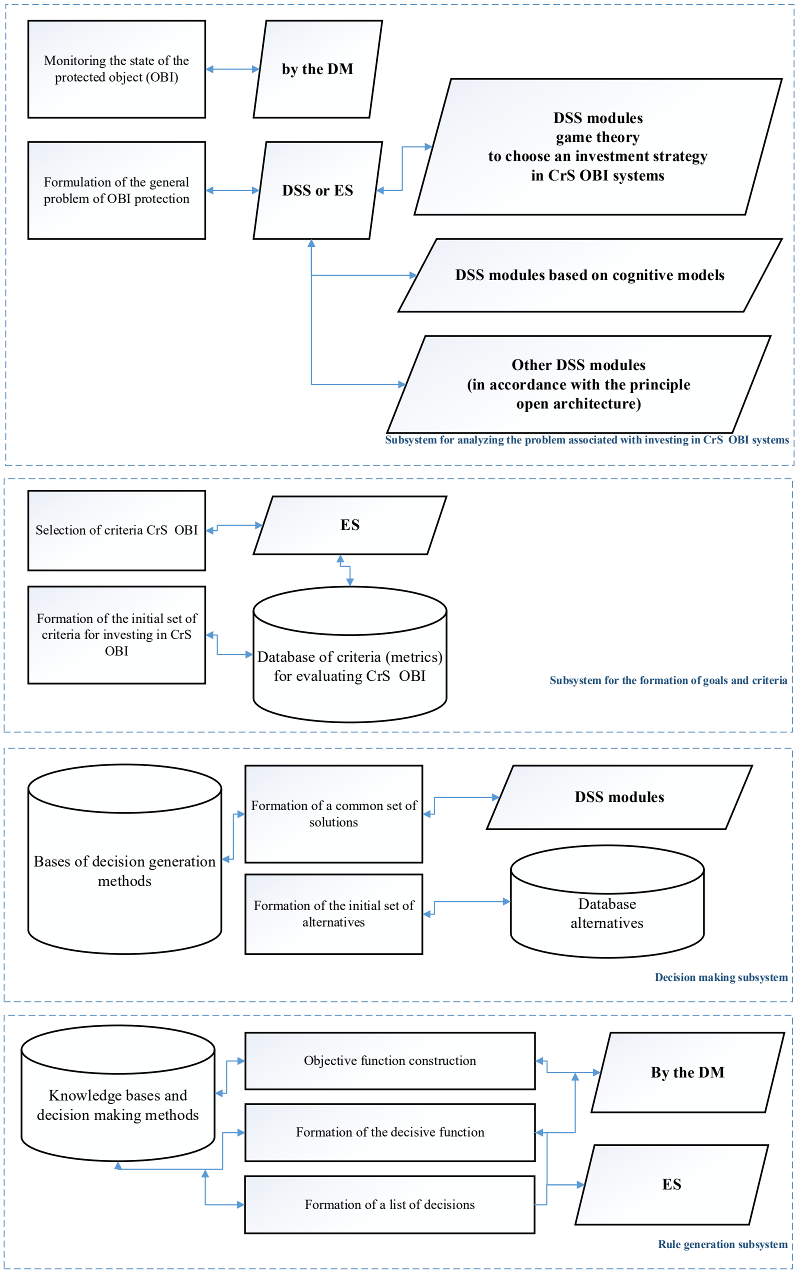

Monitoring the state of the protected object (OBI)
by the DM
DSS modules game theory to choose an investment strategy in CrS OBI systems
Formulation of the general problem of OBI protection
DSS or ES
DSS modules based on cognitive models
Other DSS modules (in accordance with the principle open architecture)
Subsystem for analyzing the problem associated with investing in CrS OBI systems
Selection of criteria CrS OBI
ES
Formation of the initial set of criteria for investing in CrS OBI
Database of criteria (metrics) for evaluating CrS OBI
Subsystem for the formation of goals and criteria
Bases of decision generation methods
Formation of a common set of solutions
DSS modules
Formation of the initial set of alternatives
Database alternatives
Decision making subsystem
Knowledge bases and decision making methods
Objective function construction
By the DM
Formation of the decisive function
ES
Formation of a list of decisions
Rule generation subsystem

Figure 1: DSS architecture in the decision-making process regarding the choice of a rational investment strategy in CrS OBI

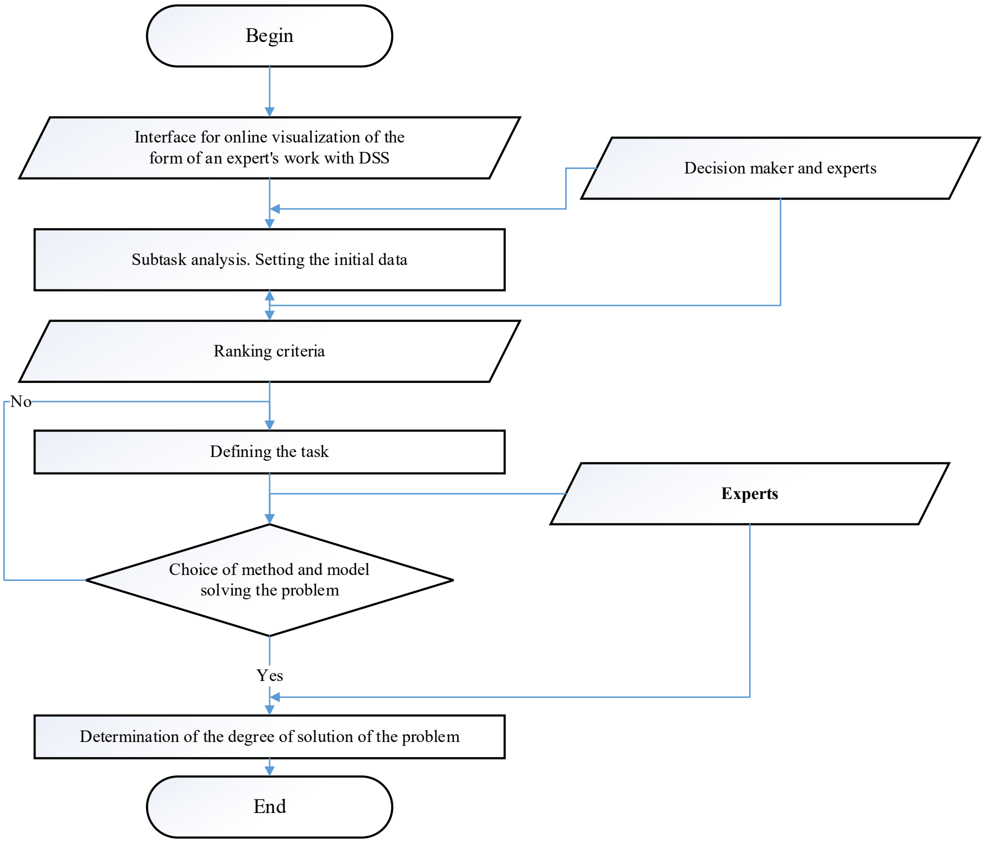

Begin
Interface for online visualization of the form of an expert's work with DSS
Decision maker and experts
Subtask analysis. Setting the initial data
Ranking criteria
No
Defining the task
Experts
Choice of method and model solving the problem
Yes
Determination of the degree of solution of the problem
End

Figure 2: Block diagram of the functioning algorithm of the subsystem "Analysis of problems and risks for an investment project in the cybersecurity systems of an informatization object"

The subsystem "Analysis of problems and risks for an investment project in cybersecurity systems of an informatization object" should provide a search and formulation of a problem with the aim of its further solution. The main directions of the functioning of this subsystem include:

monitoring of investment objects;

determination of quantitative criteria and indicators for investing in OBI cybersecurity systems;

identification of the sources of problems with the implementation of an investment project in the CrS systems of an OBI based on arguments;

the choice of the method for formulating the problem associated with investing in the CrS of the OBI;

formulation of the general problem;

determining the degree of uncertainty of the problem;

definition of individual tasks within the framework of a common problem.

After identifying the problem, it is necessary to form a list of goals and a system of criteria for the effectiveness of the implementation of an investment project in the CrS of an OBI. This is necessary for the subsequent assessment of the problem and the search for ways to further solve it.

For this, the DSS has a separate subsystem - "Formation of goals and a system of criteria for evaluating the investment strategy for the OBI cybersecurity system", see Fig. 3.

In the course of the formation of a goal or a set of goals that need to be achieved in the course of investing in CrS systems of an OBI, various tasks may arise.

These tasks can be: combined; contradict one another; be mutually exclusive, etc.

For such complex problems as the search for a rational strategy for investing in CrS systems of the object of informatization, the formation of goals and a system of criteria for evaluating the effectiveness of investment, it is advisable to divide into: fundamentally new innovative goals that are formulated by experts; typical goals, by analogy with goals that arose in similar situations; combined targets, the generation of which is available for a specific DSS.

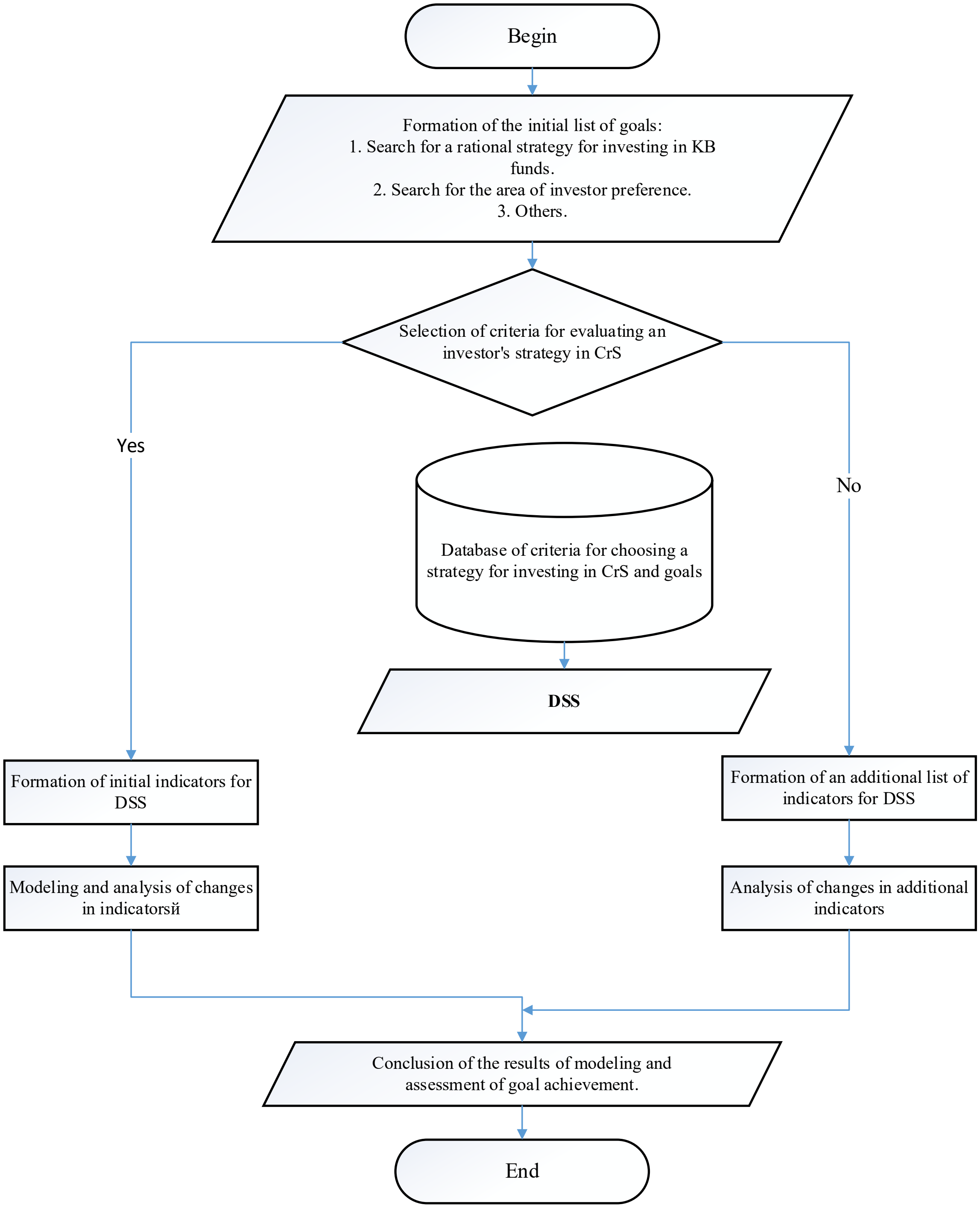

Begin
Formation of the initial list of goals:
1. Search for a rational strategy for investing in KB funds.
2. Search for the area of investor preference.
3. Others.
Selection of criteria for evaluating an investor's strategy in CrS
Yes
No
Database of criteria for choosing a strategy for investing in CrS and goals
DSS
Formation of initial indicators for DSS
Formation of an additional list of indicators for DSS
Modeling and analysis of changes in indicatorsй
Analysis of changes in additional indicators
Conclusion of the results of modeling and assessment of goal achievement.
End

Figure 3: Block diagram of the algorithm for the functioning of the subsystem "Formation of goals and a system of criteria for evaluating the investment strategy for the cybersecurity system of the object of informatization"

The most effective way to form goals and performance criteria are software systems in cooperation with experts.

The subsystem "Formation of goals and a system of criteria for evaluating an investment strategy for a cybersecurity system of an OBI" should provide a phased formation of goals and a system of criteria for the further functioning of the DSS. At the same time, this subsystem implements: a multi-level hierarchy of criteria and indicators of the effectiveness of investment in CrS systems of an OBI; the ability to decompose criteria for subgoals;

the possibility of determining the mathematical relationships between the criteria and indicators of the effectiveness of investing in CrS systems of the OBI; the ability to select scales, units of measurement, and markers for visual assessment of the investment strategy recommended by the DSS.

For further analysis of the problem of choosing a rational strategy for investing in CrS systems of an OBI, it is necessary to form alternative solutions. These alternative options will be formed in the subsystem "Formation of decisions made in the process of investing in CrS of the OBI."

The block diagram of the algorithm of functioning of the subsystem "Formation of decisions" is shown in Fig. 4.

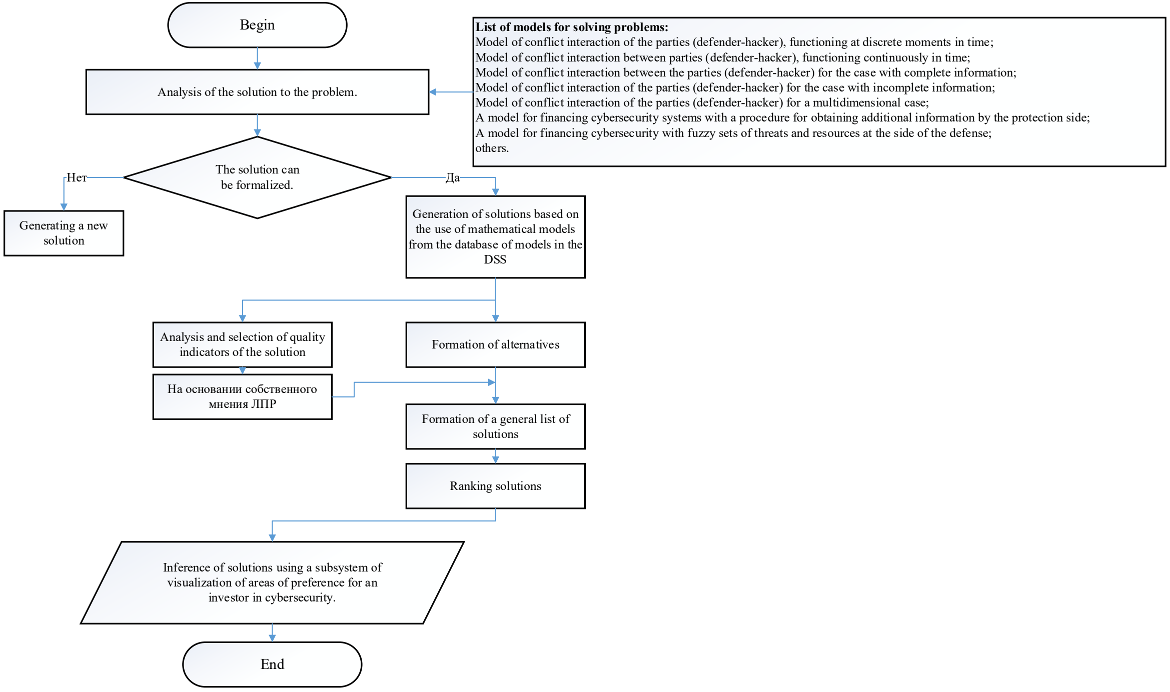

Begin
Analysis of the solution to the problem.
List of models for solving problems:
Model of conflict interaction of the parties (defender-hacker), functioning at discrete moments in time;
Model of conflict interaction between parties (defender-hacker), functioning continuously in time;
Model of conflict interaction between the parties (defender-hacker) for the case with complete information;
Model of conflict interaction of the parties (defender-hacker) for the case with incomplete information;
Model of conflict interaction of the parties (defender-hacker) for a multidimensional case;
A model for financing cybersecurity systems with a procedure for obtaining additional information by the protection side;
A model for financing cybersecurity with fuzzy sets of threats and resources at the side of the defense;
others.
The solution can be formalized.
Нет
Да
Generating a new solution
Generation of solutions based on the use of mathematical models from the database of models in the DSS
Analysis and selection of quality indicators of the solution
Formation of alternatives
На основании собственного мнения ЛПР
Formation of a general list of solutions
Ranking solutions
Inference of solutions using a subsystem of visualization of areas of preference for an investor in cybersecurity.
End

Figure 4: Block diagram of the algorithm for the functioning of the subsystem "Formation of decisions made in the process of investing in cybersecurity means of an informatization object"

The formation of possible solutions for the problems of finding rational strategies for investing in CrS systems of an OBI is currently implemented based on the use of the mathematical apparatus of game theory. The main models that are currently implemented in this subsystem are the following models [12, 18]:

conflict interaction of the parties (defender-hacker), functioning at discrete times;

conflict interaction of the parties (defender-hacker), functioning continuously in time;

conflict interaction of the parties (defender-hacker) for the case with complete information;

conflict interaction of the parties (defender-hacker) in the case of incomplete information;

conflict interaction of the parties (defender-hacker) for a multidimensional case;

financing of cybersecurity systems with a procedure for obtaining additional information by the protection side;

financing cybersecurity with fuzzy sets of threats and resources on the side of the defense;

Other.

The choice of a rational investment strategy is realized with the help of: software implementation of the analytical models presented above; using expert systems subsystems; by generating scenarios by combining different models defined by the decision maker (DM) or taken from the DSS knowledge base.

The process of forming decisions in the DSS is divided into two types: innovative solutions that the DSS is not yet able to develop (for example, the model for the situation is not yet in the knowledge base); solutions based on typical scenarios, i.e. using an analogy with known solutions.

The subsystem "Formation of decisions made in the process of investing in CrS of the OBI" provides the formation of a set of decisions in accordance with the following sequence:

generating a set of solutions using mathematical models or expert methods;

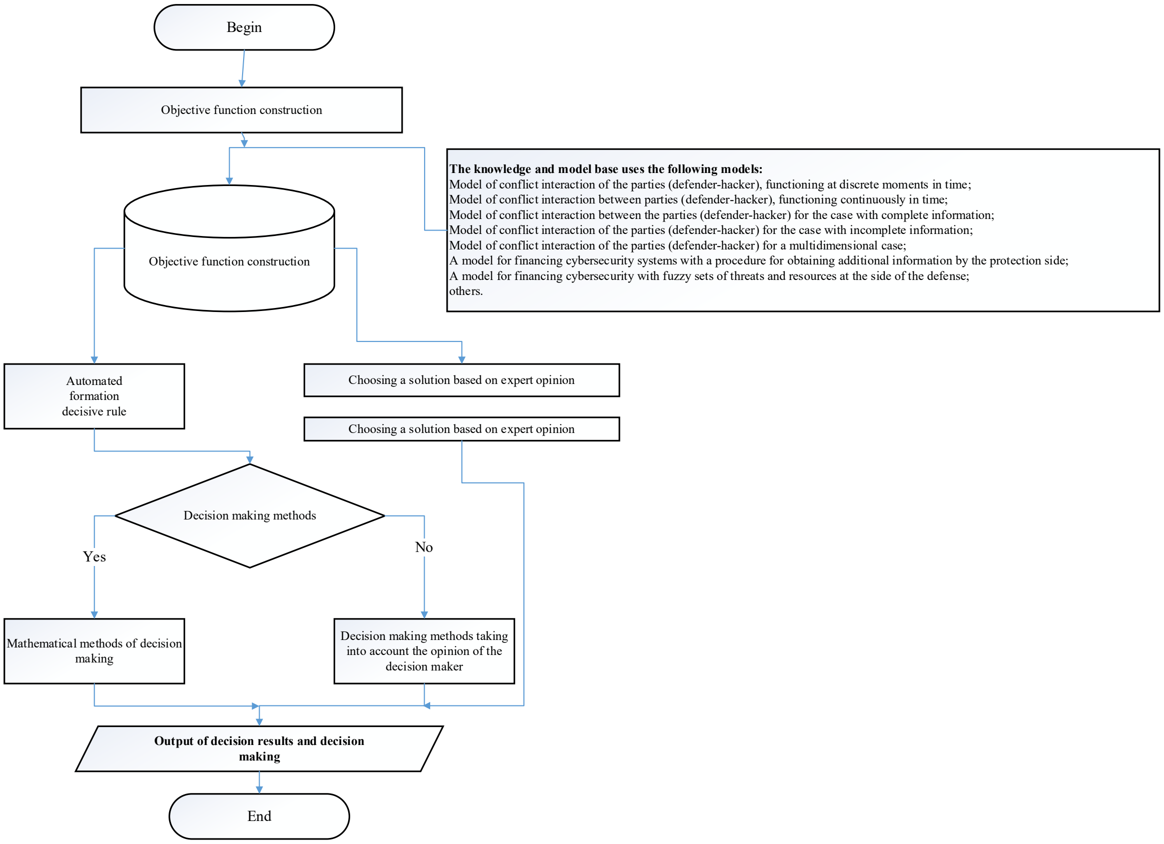
structuring alternative solutions;

3) the formation of a final subset of alternative solutions for further processing at the stage of analyzing alternatives and choosing the best solutions in the search for a rational strategy for investing in CrS systems.

The subsystem "Formation of the decision rule and analysis of alternatives in the search for a rational strategy for investing in cybersecurity systems of the object of informatization", see fig. 5 represents the following functional sequence:

1) the formation of a decision rule for choosing a solution according to the conditions of the problem. The decision-making rule is formed in an automated mode or with the involvement of a group of experts. In the latter case, it is the experts who form the decisive function depending on the investment problem, which is solved for the previously formed system of criteria. The basis for the formation of the decision rule is the multi-criteria superiority function for hierarchical structures of criteria. Also, for the decision rule, mathematical and heuristic decision support rules are important, which contribute to ensuring the choice of a rational strategy for investing in CrS systems;

2) selection of the most effective solution based on the formed decision function. The analysis and selection of alternatives in the search for a rational strategy for investing in cybersecurity systems is carried out on the basis of the formed decision rule. In the absence of a solution in the subsystem, it is possible to conduct an expert assessment of solution options. This can be done by attracting experts in the problem-oriented industry of ensuring the cybersecurity of an informatization object.


Begin
Objective function construction
Objective function construction
Automated formation decisive rule
Choosing a solution based on expert opinion
Choosing a solution based on expert opinion
Decision making methods
Yes
No
Mathematical methods of decision making
Decision making methods taking into account the opinion of the decision maker
Output of decision results and decision making
End

The knowledge and model base uses the following models:
Model of conflict interaction of the parties (defender-hacker), functioning at discrete moments in time;
Model of conflict interaction between parties (defender-hacker), functioning continuously in time;
Model of conflict interaction between the parties (defender-hacker) for the case with complete information;
Model of conflict interaction of the parties (defender-hacker) for the case with incomplete information;
Model of conflict interaction of the parties (defender-hacker) for a multidimensional case;
A model for financing cybersecurity systems with a procedure for obtaining additional information by the protection side;
A model for financing cybersecurity with fuzzy sets of threats and resources at the side of the defense;
others.

Figure 5: Block diagram of the subsystem "Formation of a decision rule and analysis of alternatives in the search for a rational strategy for investing in CrS systems of an OBI"

The formation of the decision rule is carried out together with the expert system, based on the formed knowledge base, the rule base, depending on various situations that arise during the assessment of the investment strategy.

The expert formation of the target function is implemented by organizing the interaction of experts and DSS on the basis of entering their opinions into the knowledge base.

The subsystem "Formation of the decision rule and analysis of alternatives in the search for a rational strategy for investing in cybersecurity systems of the object of informatization" allows building a decision function both in an automated mode and on the basis of taking into account expert opinions. The independent application of the rules makes it possible to compare the initial solutions and the solutions obtained as a result of their functioning of this subsystem.

The DSS expert subsystem is one of the main applications of artificial intelligence and is designed to solve problems related to a specific subject area, knowledge about which is stored in the knowledge base.

The main purpose of the expert subsystem, as the basis of a DSS for finding a rational strategy for investing in cybersecurity systems of an informatization object, is to focus on solving various problems, based on the models previously described in [12, 18].

The block diagram of the algorithm for the functioning of the expert subsystem is shown in Fig. 6.

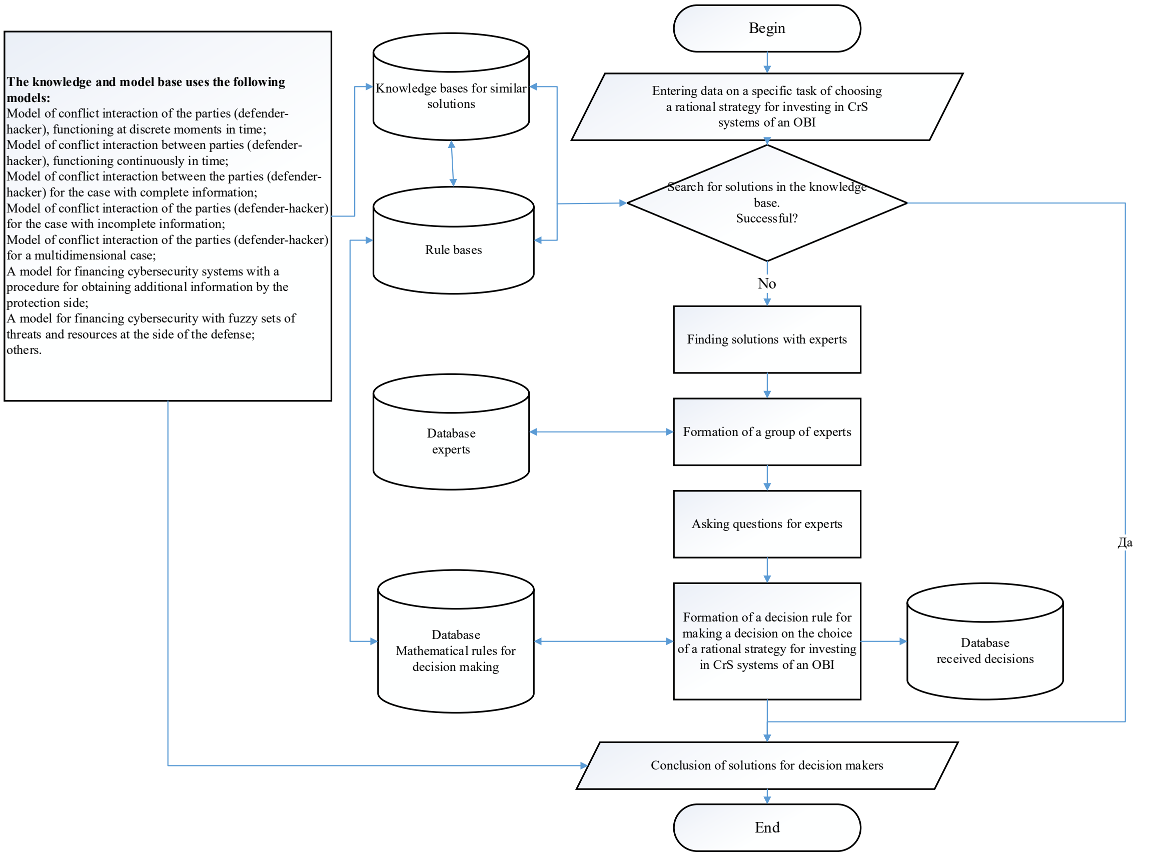

The knowledge and model base uses the following models:
Model of conflict interaction of the parties (defender-hacker), functioning at discrete moments in time;
Model of conflict interaction between parties (defender-hacker), functioning continuously in time;
Model of conflict interaction between the parties (defender-hacker) for the case with complete information;
Model of conflict interaction of the parties (defender-hacker) for the case with incomplete information;
Model of conflict interaction of the parties (defender-hacker) for a multidimensional case;
A model for financing cybersecurity systems with a procedure for obtaining additional information by the protection side;
A model for financing cybersecurity with fuzzy sets of threats and resources at the side of the defense;
others.
Knowledge bases for similar solutions
Rule bases
Database experts
Database Mathematical rules for decision making
Begin
Entering data on a specific task of choosing a rational strategy for investing in CrS systems of an OBI
Search for solutions in the knowledge base. Successful?
No
Да
Finding solutions with experts
Formation of a group of experts
Asking questions for experts
Formation of a decision rule for making a decision on the choice of a rational strategy for investing in CrS systems of an OBI
Database received decisions
Conclusion of solutions for decision makers
End

Figure 6: Block diagram of the operation algorithm of the expert subsystem for the designed DSS

The expert subsystem provides the development and assessment of possible alternatives for investing in the CrS systems of the OBI by the user using the knowledge that was obtained from expert specialists.

The expert subsystem consists of:

KB, which is designed to store the initial and intermediate facts accumulated in the course of solving the problem. Also, the knowledge base stores models and rules for manipulating models. It is also possible to design a separate rule base if there are a lot of rules used in the process of solving the problem of choosing a rational strategy for investing in cyber security systems;

block for solving problems associated with the choice of a rational investment strategy from the cybersecurity system. This block will ensure the implementation of the sequence of rules execution for solving a specific investment task based on the criteria and rules stored in the database and the knowledge base;

an explanatory subsystem that will allow the decision maker to understand the reason for such a solution, which is proposed by the DSS;

a module for generating rules, which is designed to add new rules to the knowledge base and / or modify them;

dialogue interface, which is designed to implement a convenient user dialogue with the subsystem and the DSS, in general.

The sequence of actions of the functioning of the algorithm shown in Fig. 6 is as follows.

Upon receipt of information about tasks, a solution is sought in the existing knowledge base. If a similar situation was encountered earlier and the rules for making decisions were determined, then the solution for this problem is also uniquely determined.

If there is no solution for the initial formulation of the problem, then a problem-oriented expert group is formed. Further, questions are sent to experts that will help form a new decision rule in the future. Experts form a decision rule for choosing the best alternative and the corresponding DSS subsystem.

At the next stage, the choice of the best solution is determined. If the solution corresponds to the original formulation of the problem, the rule is recorded in the database of rules, and the solution in the knowledge base.

This algorithm for the functioning of the DSS (or ES) provides the ability to analyze and find a solution for any problem associated with choosing a strategy for investing in CrS systems of an OBI.

4. COMPUTATIONAL EXPERIMENT TO FIND RATIONAL STRATEGIES FOR INVESTORS IN CYBERSECURITY SYSTEMS OF OBJECTS OF INFORMATIZATION

To visualize the results obtained using the results described in the previous paragraphs of the article in the DSS, the Plotly library for the Python language was used. Calculations were carried out for investment projects in various investment projects in the field of cybersecurity in Ukraine and Kazakhstan [11].

Some of the results obtained in the process of multidimensional modeling of investment strategies in the CrS of an OBI using an online DSS are shown in Figures 7-9.

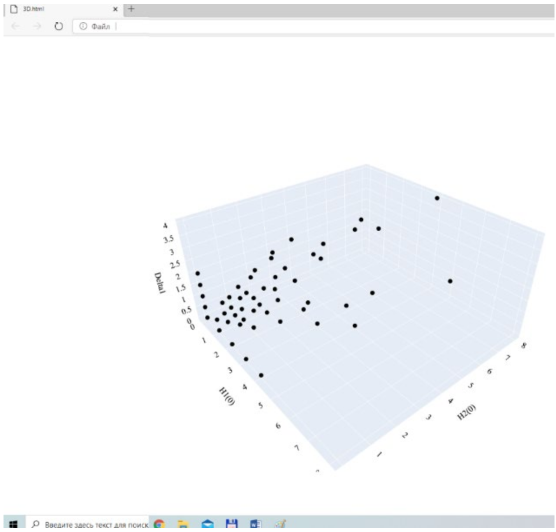


Figure 7: Dependence of the preference set for the security side of the informatization object for 3 variables

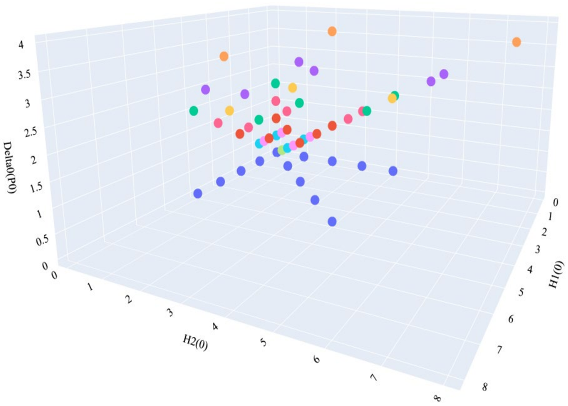


Figure 8: Dependence of the preference set for the security side of the informatization object for 4 variables

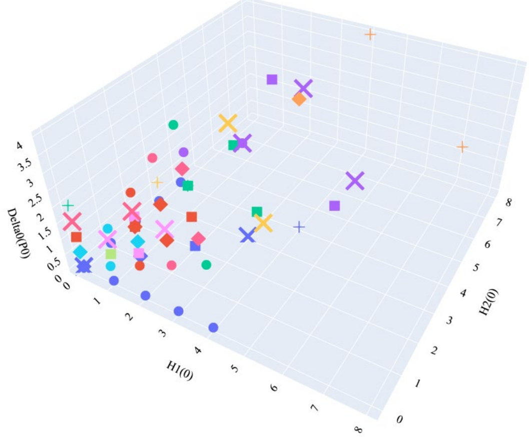


Figure 9: Dependence of the preference set for the security side of the informatization object for 5 variables

5. DISCUSSION OF THE RESULTS OF THE COMPUTATIONAL EXPERIMENT

The obtained results of experimental calculations show the effectiveness of the proposed toolkit for solving the problem of continuous management of financial resources of investors in the CrS systems of the OBI of the parties, taking into account the multifactorial nature of this task.

Figure 7 shows a collection of points in three-dimensional space, which reflects the following situation. For each point corresponding to the financial resources of the defense side (axis H1 (0)), the value of the financial resources of the opposing party (i.e., a hacker, axis H2 (0)) is given. The Delta (P0) parameter characterizes the degree of reliability of the data on the financial resources of the parties spent on bringing the dynamic system to its terminal surface.

There can be several values of H1 (0), H2 (0), Delta (P0). Some of these values correspond to a set that guarantees the continuation of the procedure for investing in projects related to the CrS of an OBI, and some correspond to a set in which a hacker cannot continue investing in an attack on an informatization object. Then, choosing from these values the minimum (for each component), we obtain for each value of the financial resource of the security side of the informatization object a set that will belong to the preference set of the defender of the informatization object. It should be noted that the graphical interpretation depicting a set of points for the graphs of the online DSS platform will correspond to the model of investing in cybersecurity systems of the informatization object, in which it is assumed that the defender can use his financial resources (FR), determined by the specified sets of these resources (antiviruses, firewall, systems of cryptographic protection of information, etc.). These sets of FR can be determined by the choice of specific investment programs in the CrS systems of the OBI.

As in Figure 7, Figure 8 also shows sets of points that characterize the financial resources of the defender and the hacker. The essence of the interpretation for both Figure 8 and Figure 7 remains the same. However, we note that the choice of this method of illustration of the set of preferences of the defender of the informatization object makes it possible to graphically illustrate in spaces of greater dimension than three. This circumstance is a positive point in the developed DSS.

Unfortunately, it is impossible to use more than three dimensions directly. However, a workaround was found for the online DSS platform. For example, for 4.5 and 6-dimensional plots, using the Plotly library for the Python language, you can emulate the rendering depth by varying the colors, size or shape of the markers. In Figure 8, the light shade of the markers will correspond to the lower values of the cost of the hacker's financial resource to overcome the boundaries of protection of the OBI.

Figure 9 serves as an additional confirmation of the possibility of graphic interpretation in spaces of greater dimensions than three or even four. The essence of the interpretation is the same as for Figure 7.

The size of the marker for Figure 9 makes it possible to use the visualization of the fifth dimension. Here's the markersize parameter of the Scatter3D function for the Plotly library applied. Forms of markers are suitable for visualizing categories of projects within the framework of different strategies for investing in CrS systems of an OBI. For example, round markers correspond to the category of projects for the development of antivirus protection, diamonds - cryptographic protection systems, (+) - intrusion detection systems, etc. The Plotly library provides a choice of 10 different shapes for 3D graphs. Thus, up to 10 different values can be shown as a marker form for the online DSS platform.

Comparing the available models described in [12-20], our proposed model shows improved parameters of efficiency and predictability for an investor in CrS systems of an OBI by an average of 8-11%. The data were obtained on the basis of comparing the results of modeling using an online DSS platform and the results of real returns from several investment projects in the CrS systems of enterprises and organizations in Ukraine and Kazakhstan.

It seems promising to further study the presented models of the computational core of the DSS for solving problems in the field of investment within the framework of a fuzzy information scheme, for example, in industrial, defense and other sectors of the economy.

The identified drawback of the model is the fact that the forecast assessment data obtained using the online DSS platform did not always coincide with the actual data when choosing strategies for investing in cybersecurity systems of the informatization object. However, this was influenced by the difficult economic situation, not least related to the drop in business activity of investors in the context of the Covid-19 coronavirus pandemic.

Note that in comparison with the existing models [10-20], the proposed solution improves predictability indicators for an investor in the CrS system of an OBI.

As a solution to the problem of improving the efficiency of investment in information security of enterprises, we propose a new approach based on an ensemble of models that form the core of an intelligent information system, which allows you to perform a comprehensive assessment of the costs of information security. This approach is implemented as a software package.

Further prospects for the development of this study, set out in the framework of the article, is the transfer of the accumulated experience into the real practice of optimizing the investment policy of the cybersecurity system of public and private companies in other countries.

6. ACKNOWLEDGMENTS

The research and article were carried out within the framework of the grant of the Republic of Kazakhstan registration number AP08855887-OT-20 "Development of an intelligent decision support system in the process of investing in cyber security systems."

7. CONCLUSION

The authors of the article propose a structural diagram of the functioning of the DSS in the process of analyzing and choosing a rational (optimal) strategy for investing in cybersecurity systems (CrS) in a dynamic confrontation with the opposing side (hacker) The key functional modules of such a DSS are considered, which contribute to ensuring the continuous and efficient functioning of the system. Detailed block diagrams are given for the following key subsystems of this DSS:

a subsystem for analyzing the problem, risks and threats associated with insufficient investment in CrS systems of an informatization object (OBI);

a subsystem for the formation of goals and criteria for assessing the effectiveness of investment in CrS systems of an OBI;

decision making subsystem;

a subsystem for forming a decision rule and analyzing alternative strategies for investing in cybersecurity systems of an OBI.

The above scheme provides full-featured decision-making in the process of choosing rational strategies for investing in cybersecurity systems of objects of informatization of any scale, from small companies or enterprises to large OBI.

REFRENCES:

[1] Mohammadhassani, A., Teymouri, A., Mehrizi-Sani, A., & Tehrani, K. (2020, June). Performance Evaluation of an Inverter-Based Microgrid under Cyberattacks. In 2020 IEEE 15th International Conference of System of Systems Engineering (SoSE) (pp. 211-216). IEEE.

[2] Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2020). Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. arXiv preprint arXiv:2006.11929.

[3] Gordon L.A., Loeb M.P. (2002). The Economics of Information Security Investment. ACM Transaction on Information and System Security, Vol. 5, No 4, pp. 438-457.

[4] Sokolov, S., Nyrkov, A., Knysh, T., & Shvets, A. (2020, December). Countering Cyberattacks During Information Operations. In Proceedings of the XIII International Scientific Conference on Architecture and Construction 2020 (pp. 84-100). Springer, Singapore.

[5] Yaacoub, J. P. A., Salman, O., Noura, H. N., Kaaniche, N., Chehab, A., & Malli, M. (2020). Cyber-physical systems security: Limitations, issues and future trends. Microprocessors and Microsystems, 77, 103201.

[6] Philp, D., Chan, N., & Sikos, L. F. (2020). Decision support for network path estimation via automated reasoning. In Intelligent Decision Technologies 2019 (pp. 335-344). Springer, Singapore.

[7] Lakhno, V. A., Kasatkin, D. Y., Blozva, A. I., Kozlovskyi, V., Balanyuk, Y., & Boiko, Y. (2020, October). The Development of a Model of the Formation of Cybersecurity Outlines Based on Multi Criteria Optimization and Game Theory. In Proceedings of the Computational Methods in Systems and Software (pp. 10-22). Springer, Cham.

[8] Simon, J., & Omar, A. (2020). Cybersecurity investments in the supply chain: Coordination and a strategic attacker. European Journal of Operational Research, 282(1), 161-171.

[9] Hallman, R. A., Major, M., Romero-Mariona, J., Phipps, R., Romero, E., John, M., & Miguel, S. (2020, May). Return on Cybersecurity Investment in Operational Technology Systems: Quantifying the Value That Cybersecurity Technologies Provide after Integration. In COMPLEXIS (pp. 43-52).

[10] Farao, A., Panda, S., Menesidou, S. A., Veliou, E., Episkopos, N., Kalatzantonakis, G., ... & Xenakis, C. (2020, September). SECONDO: A platform for cybersecurity investments and cyber insurance decisions. In International Conference on Trust and Privacy in Digital Business (pp. 65-74). Springer, Cham.

[11] Akhmetov, Bakhytzhan, et al. 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. p. 162-171.

[12] Akhmetov, B. B., et al. (2018). The choice of protection strategies during the bilinear quality game on cyber security financing. *Bulletin of The National Academy of Sciences of the Republic of Kazakhstan*, (3), 6-14.

[13] Gordon, L. A., Loeb, M. P., & Zhou, L. (2016). Investing in cybersecurity: insights from the Gordon-Loeb model. *Journal of Information Security*, *7*(02), 49.

[14] Kelly, B. B. (2012). Investing in a centralized cybersecurity infrastructure: Why hacktivism can and should influence cybersecurity reform. *BUL Rev.*, *92*, 1663.

[15] Kosutic, Dejan, and Federico Pigni. "Cybersecurity: investing for competitive outcomes." *Journal of Business Strategy* (2020).

[16] Direction, Strategic. "Investing in cybersecurity: Gaining a competitive advantage through cybersecurity." (2020).

[17] Panaousis, E., Fielder, A., Malacaria, P., Hankin, C., & Smeraldi, F. (2014, November). Cybersecurity games and investments: A decision support approach. In *International Conference on Decision and Game Theory for Security* (pp. 266-286). Springer, Cham.

[18] Lakhno, V., Malyukov, V., Gerasymchuk, N., & Shtuler, I. (2017). Development of the decision making support system to control a procedure of financial investment. Eastern European Journal of Advanced Technologies, (6 (3)), 35-41.

[19] Rea-Guaman, M., Calvo-Manzano, J. A., & San Feliu, T. (2018, June). A prototype to manage cybersecurity in small companies. In *2018 13th Iberian Conference on Information Systems and Technologies (CISTI)* (pp. 1-6). IEEE.

[20] ZibIn, S. V. (2017). PIdsistemi I modulI sistemi pIdtrimki priynyattya rIshen. Algoritmi funktsIonuvannya. TelekomunIkatsIynI ta InformatsIynI tehnologIYi, (4), 58-70.