***Визначено основні концепції, що формують основу інтегрованого моделювання поведінки антагоністичних агентів в системах кібербезпеки. Показано, що значною мірою акцент робиться на моделюванні поведінки тільки однієї зі сторін кіберконфлікта. У тому випадку, коли розглядається взаємодія всіх сторін конфлікту, підходи, що використовуються, орієнтовані на рішення часткових завдань, або моделюють спрощену ситуацію.***

***Пропонується методологія моделювання взаємодії антагоністичних агентів в системах кібербезпеки, яка орієнтована на використання мультімодельного комплексу з елементами когнітічного моделювання. Для цього виділені основні компоненти кіберконфлікта, моделі яких повинні бути розроблені. Моделювання взаємодії антагоністичних агентів пропонується реалізовувати як моделювання ситуацій. Сформульовано поняття ситуації і наведены її компоненти.***

***У запропонованій методології традиційні методи і інструменти моделювання не протиставляються один одному, а розглядаються в сукупності, формуючи тим самим єдину методологічну базу моделювання поведінки антагоністичних агентів.***

***У пропонованих до використання мультімодельних комплексах, окремі елементи та їх функції досліджуваного об'єкта описуються за допомогою різних класів моделей на певному рівні деталізації. Координоване застосування різних моделей дозволяє підвищити якість моделювання за рахунок компенсування недоліків одних моделей перевагами інших, зокрема відображення динаміки взаємодії в системно-динамічних і агентнах моделях, що ускладнено в класичних моделях теорії ігор.***

***Мультімодельние комплекси дозволяють сформувати концепцію «віртуального моделювання». Ця концепція дозволяє проводити моделювання з використанням моделей різних класів, які повинні відповідати цілям і завданням моделювання, характеру та структурі вихідних даних.***

***В результаті досліджень пропонується методологія моделювання взаємодії антагоністичних агентів в системах кібербезпеки з використанням методів на основі запропонованих моделей рефлексивної поведінки антогоністіческіе агентів в умовах сучасних гібридних загроз***

***Ключові слова: кібербезпека, антагоністичні агеніти, методологія моделювання, системна динаміка, рефлексивний агент, мультиагентні системи, когнитивне моделювання***

UDC 681.32:007.5
DOI: 10.15587/1729-4061.2019.164730

# DEVELOPMENT OF METHODOLOGY FOR MODELING THE INTERACTION OF ANTAGONISTIC AGENTS IN CYBERSECURITY SYSTEMS

**O. Milov**
PhD, Associate Professor*
E-mail: Oleksandr.Milov@hneu.net
**A. Voitko**
PhD, Head of Research Laboratory
Research Laboratory of Information Security Issues
Department of Information Technology and Information Security Employment
Institute of Information Technologies
National University of Defense of Ukraine named after Ivan Chernyakhovsky
Povitroflotskiy ave., 28, Kyiv, Ukraine, 03049
**I. Husarova**
PhD, Associate Professor
Department of Applied Mathematics
Kharkiv National University of Radio Electronics
Nauky ave., 14, Kharkiv, Ukraine, 61166
**O. Domaskin**
PhD
Department of Economic Cybernetics and Information Technologies
Odessa National Economic University
Preobrazhenska str., 8, Odessa, Ukraine, 65082
**E. Ivanchenko**
PhD, Associate Professor***
**I. Ivanchenko**
PhD***
**O. Korol**
PhD, Associate Professor
Department of Information Systems**
**H. Kots**
PhD, Associate Professor*
**I. Opirskyy**
Doctor of Technical Sciences
Department of Information Security
Lviv Polytechnic National University
S. Bandery str., 12, Lviv, Ukraine, 79013
**O. Fraze-Frazenko**
PhD, Associate Professor
Department of Automated Systems and Cybersecurity
Odessa State Academy of Technical Regulation and Quality
Kovalska str., 15, Odessa, Ukraine, 65020
*Department of Cyber Security and Information Technology**
**Simon Kuznets Kharkiv National University of Economics
Nauky ave., 9-A, Kharkiv, Ukraine, 61166
***Department of Information Technology Security
National Aviation University
Kosmonavta Komarova ave., 1, Kyiv, Ukraine, 03058

## 1. Introduction

Computer simulation is of great importance in the field of cybersecurity. Simulation is useful as components of network security software, in training exercises for security professionals, and as software tools designed for network users. Moreover, much of the basic research in the field of human factor and cyber epidemiology is associated with the use of

simulation software. The dynamics of cybersecurity is mainly human and opposing, encompassing a number of interactions between the attacker, the defender and the user [1]. Modeling the characteristics and behavior of individuals included in the cybersecurity system is of particular importance for considering the characteristics of this subject area.

The challenges of controlling cybersecurity systems are initially interdisciplinary. Decisions at the strategic level (for example, planning investments in the development of countermeasures) are closely related to decisions at the tactical and operational levels (for example, forecasting cyber threats and operational planning of protective measures).

It is wrong to speak about the model in general when mathematical modeling of complex systems, such as cybersecurity systems. There are always a set of models, each of which is able to provide an answer to very specific questions about the behavior of both the attacker and the defender, and each of these models has its own mathematical structure.

Solving complex interconnected management problems with the help of any one method of modeling, as a rule, leads to inconsistent model fragments and far from reality problem statements that do not provide any support for decision making in controlling cybersecurity systems.

As a rule, the real tasks of ensuring the required level of protection of objects of critical infrastructure require the simultaneous use of various concepts, tools and models of decision-making support. This is due, firstly, to the complexity of managing the cyber defense system, secondly, simultaneous solution of control tasks in various structures of the cybersecurity system (technological, organizational, functional, informational, program, technical, financial), and thirdly, changing control tasks, the structure and completeness of the source and output data in the dynamics under hybrid threats.

Cybersecurity systems operate under conditions of uncertainty, characterized by a lack of information necessary to formalize the processes occurring in them. Uncertainty is due, on the one hand, to the insufficiency or complete lack of methods and means of determining the state of the parties to the conflict, and on the other, ignorance of the laws governing the processes due to their complexity and little knowledge. These factors lead to the impossibility of an analytical description and construction of formal models that take into account the specifics of cybersecurity systems, which, in turn, significantly reduces the effectiveness of controlling these systems in the context of hybrid threats.

As a result, the role of the decision maker (DM) increases dramatically, who in the case when traditional methods of control, mathematical description or management do not give the desired results, copes with the task with a certain degree of efficiency, relying on the ideas and knowledge of experts in this field and own experience and intuition.

Thus, a subjective factor makes a significant contribution to the DM decision. In addition, in cyber security systems, it affects not only the adoption, but also the result of the impact of management decisions, since a significant part of these impacts is also directed at the person, who is an integral part of these systems. In this regard, it is necessary to take into account the formalization of the processes of counteraction in the conditions of cyber conflicts, peculiarities caused by human behavior. Therefore, when building a formal model, it is advisable to use methods based on reproducing the intellectual activities of the decision maker. They allow reducing the degree of subjectivity of the decisions made and, as a result, increase the efficiency of system control.

All this leads to the need to develop a methodology for modeling not only the processes ensuring the cybersecurity of objects of critical infrastructure, but also, first and foremost, behavior in the process of interaction of cyber conflict participants.

## 2. Literature review and problem statement

In [2], it is shown that network simulations for effective use should include highly accurate models of users, intruders and/or defenders. Simulations can be used to implement scripts for learning war games with realistic traffic and user-generated vulnerabilities. The collection and analysis of data from these simulations provides an opportunity to explore how various changes in tools, security constraints, and training can affect the overall network security. Modeling the behavior of users and defenders can be used to assess their cognitive states in real time. Models of learning and adapting the behavior of cyber conflict participants can be used in combination with the theory of behavioral games to predict possible attack scenarios and select the best defenses [3, 4]. Modeling user network activity allows testing various network policies without real consequences. Such modeling can be used to identify potential vulnerabilities in procedures and currently used cyber security practices [5].

Models of learning processes and behavior can help better understand the intentions of cyber attackers, defenders and users, which will significantly increase the level of network security. The research results presented in [6, 7] show that modeling and predicting the mental state and decisions of intruders can lead to an improvement in decision-making methods for preventing attacks. The psychological state of participants in cyber conflict, their stress susceptibility, attitude to risk are ignored by the authors of most publications describing cybersecurity tools.

Recently, not only cyber wars, but also individual cyber threats have acquired a hybrid character, which increased the level of threats by an order of magnitude compared with previous years. This implies that countermeasures also have to adapt to appropriate changes, using together all possible countermeasures in a coordinated manner. However, in most of the works describing cybersecurity tools, the emphasis is on the technical side of cyber conflict. At the same time, the psychological and behavioral aspects of the participants in the cyber conflict are ignored. Consideration of these aspects of only one of the conflict parties does not allow achieving a synergistic effect from the use of simulation results. This effect occurs only when we jointly consider the behavior of the «attacker – defender – user» triad.

Studies show that using the results of modeling the behavior of all participants in a cyber conflict can significantly improve the efficiency of decision-makers in security systems.

Currently, methods for predicting the behavior of network users are largely based on statistical analysis. This approach was proposed in [9, 10], the main findings of which demonstrate that, even limited to determining the correlation between factors of cyber conflict, it is possible to increase the effectiveness of training defenders/users of information systems.

It is argued in [11] that ensuring the information security of cyber systems and information technologies should be focused on the «confidentiality – integrity – accessibility» triad. The security of information technologies in conditions

of hybrid cyber threats in cyberspace includes a wide range of activities and interactions. Increasing the activity of participants in communication, collaboration and similar types of activities affects and significantly affects all aspects of information security. In fact, security is a process, and not a product, which conceptually cannot be limited to the specified triad. Additional characteristics of authenticity, accuracy, usefulness and access rights are combined and encompass the ways of access, ownership and reliability of data between services and organizations. In [12], it was shown that this approach provides a more complete conceptualization of information security. In addition, the process of information security requires an understanding of the psychology of people, their behavior, strategies, tools and methods [13]. Modern cybersecurity operates with concepts, strategies, approaches and risk management tools. Best practices protect information and parties involved from all forms of malicious influence (physical, financial, emotional) resulting from a security breach.

Cybersecurity technical solutions are and should be seen as crucial to the success of security efforts. The use of encryption in communications, access control methods, as well as monitoring and auditing tools, of course, reduces the damage to the security of computer systems, and provides some protection against attacks. It should be borne in mind, as shown in [14], that it is the participants of a cyber conflict that may be the most vulnerable from the point of view of security, and human factors must be considered from the point of view of security.

In fact, the characteristics of the functions performed, determined by human factors, can lead to the destruction of even the best intentions to ensure cybersecurity. [15] addresses deliberate and unintentional internal threats to cybersecurity. Unintentional insider threat applies to cases where the administrator may not be able to properly configure the server or the user becomes a victim of a phishing email for good intentions. The attacks of social engineering, provoked by an external party, can lead to the fact that employees inadvertently create an insider threat. To be better prepared and equipped to prevent cyber incidents, an organization must take into account both the technical security elements when designing systems and networks, and the cultural and social aspects of personnel management. Ideally, following good cybersecurity practices should integrate cybersecurity knowledge, awareness, and models for assessing situations in an organizational culture, both when designing and operating a system. Regardless of the quality of cybersecurity technical solutions, vulnerability analysis often covers organizational issues related to the lack of funding for staff training or support from management. The lack of attention to the analysis of the human factor (poor communication and lack of training) undermines security efforts.

The human factors of cybersecurity require a balance between usability and utility of software systems, as well as the policies and constraints imposed on them in terms of security.

Assume that perimeter protection tools and methods, such as firewalls, intrusion detection systems (IDS), filters, and network monitoring methods, are absolutely effective. But even in this case, human behavior, deliberate or otherwise, can become a bridge through these means of protection and disrupt security. That is why human behavior is a key issue in the theory and practice of security, as demonstrated in [16, 17].

The behavior of individuals related to the cybersecurity system is important not only to understand, but also to model in order to predict the possible consequences in many areas of cybersecurity. As tools for analyzing and simulating the behavior of participants in a cyber conflict, the researchers point out methods of dynamic prosecution games [18, 19], reflexive behavior [20–22], evaluating cyber threats [23, 24], team decision-making [25], and others. Recently, human factors have become a matter of primary importance for the network security community [26–28].

It should be noted that in the conditions of the formation of a new class of hybrid threats, the cybersecurity area requires urgent measures to use the entire arsenal of modeling tools to ensure the necessary level of cybersecurity. Analysis of the literature demonstrated that, despite the diversity of approaches, a huge range of models and methods, most of them are aimed at analyzing and developing software and hardware protection tools, and in the case of modeling the behavioral aspects of participants in a cyber conflict, the models reflect only one of the parties without interaction with the enemy [6]. Moreover, these publications relate to the period preceding the emergence of hybrid threats that have significantly changed the nature of the confrontation in cyberspace. At present, there is no theoretical model covering all or at least the main aspects of the process of antagonistic interaction of agents in cybersecurity systems. Moreover, none of the scientific disciplines studying the process of communication, considers the process of confrontation as a whole. To a certain extent, within the framework of artificial intelligence, the processes of interaction (communication) are considered and the process of communication is modeled with significant limitations. In this case, as follows from [29], the main attention is paid to analyzing and modeling the behavior of an individual agent, understanding the agents' communication processes, which has the nature of cooperation. This approach determines a significant number of publications on the problems of agent coordination in the process of functioning. In the case when the interaction of agents in a state of conflict is considered (a condition involving a struggle that should lead to its resolution), the designed mathematical models are fairly formal, and their implementation in a particular subject area is not always obvious [30].

Currently, the following basic approaches (methods) dominate to model the interaction of individuals in the field of cybersecurity.

1. System dynamics. System dynamics uses a combination of linear and non-linear first-order difference equations to relate qualitative and quantitative factors. The system-dynamic approach is based on the principles developed by Forrester to study dynamic processes using control principles [31, 32]. System-dynamic models are mini-theories of real systems that «must not only reproduce/predict behavior, but also explain how behavior is formed» [33]. Consequently, the method of system dynamics is qualitative and quantitative modeling and, at the same time, an analysis of the dynamics of real systems.

The stages of qualitative analysis of the system-dynamic modeling process [34] are conceptualization and formulation of the model. These stages help to get an idea of the complex dynamics between the attackers and the defenders described in the theoretical framework. At the qualitative stage, a systematic review of the literature [35] on the interaction of antagonistic agents in security systems is carried out. The system dynamics tools are then used to visually present the concepts. The tools for conceptualizing the model and guiding it are the stock, flow and cause-and-effect diagrams.

Thus, the stock and flow, as well as cause-and-effect diagrams, obtained as a result of a qualitative study, are parame-

terized within the framework of a quantitative model. The run of the quantitative model allows checking and analyzing the behavior of agents generated in accordance with the basic assumptions [36].

2. Process (discrete-event) simulation. This type of modeling is a description of the processes occurring in the system, described as a sequence of transactions (processing of detection signals, documents, response to incoming information, etc.). This type of simulation can be considered as a way of describing the operation of queuing systems (QS) of any complexity. Process models are presented in the form of blocks processing applications (transactions), and the connections between the blocks are determined by the sequence of operations to be executed.

3. Game simulation, which is based on the basic concepts of game theory: strategy, payment matrix, coalition, etc. The game-theoretic approaches applied to solving information security problems can be divided into 2 classes. The first class describes the «attack – defense» interaction, predicting the actions of the attackers and determining the response actions of the defense. The second class allows obtaining quantitative estimates of the level of protection of the information system by predicting the actions of attackers and defenders. Game-theoretic methods are widely used in the problems of designing intrusion detection systems (IDS). At the same time, the issues of counteracting attacks aimed at the IDS itself did not receive proper research from the standpoint of game theory.

At the end of the twentieth century, the theory of network games began to actively develop. This section of game theory specializes in the formation of stable network structures that reflect the connections formed between players in the context of diverging interests and different awareness of players. The use of this type of game simulation should be considered promising for modeling the interaction of antagonistic agents [37, 38].

In the case of interaction between players, the result of their interaction is determined by one or another «network» (graph-theoretic) model. In this case, an adequate simulation method is the «network games» class, which includes «cognitive games» and «games on social networks». In the first case, a cognitive map is used to take into account causal relationships and the interaction of factors, as well as to simulate the dynamics of non-formalizable systems [39]. In the second case, the vertices are agents participating in the social network, and weighted arcs reflect the degree of their «trust» to each other. The opinion of each agent is influenced by initial opinions and the opinions of other agents, taking into account their trust to each other. In addition to agents, there are players in the model who can influence agents and their interaction.

4. Agent modeling – a method of describing a system as a set of independent entities, each of which can follow its own rules, interact with each other and with their environment. Various constructions can be used to define agent models, including a program code, but finite automata are the most convenient way to specify the agent's behavior.

Agent-based models have a wider range of applications and are used from the physical level of abstraction to the strategic. However, it is a mistake to think that models are a replacement for discrete-event and system-dynamic models. Agent-based models are much more complicated, more diverse, and allow you to model the behavior of agents, given their activity.

The complexity and uncertainty of cybersecurity systems are largely due to the interaction of active network elements. In this regard, the involvement of the multi-agent systems approach as an ideology of conceptual, mathematical, and simulation modeling based on intelligent agents seems appropriate.

Based on the results of the analysis of publications relating to the period of the emergence of hybrid cyber threats of a new generation, we can draw the following conclusions.

1. The main part of publications related to the modeling of processes in cybersecurity systems is primarily aimed at reviewing the software and technological aspects of the functioning of such systems.

2. Publications examining the behavior of participants in cyber conflict focus on the behavior of individual parties to the conflict, rather than on their interaction. In the case of considering the interaction of antagonistic agents, the proposed models describe the interaction as a one-step act (game-theoretic models), and the choice of strategy is reduced to a one-time determination from the set of already formed pure or mixed ones. There is no change of strategies in the process of interaction, therefore such models describe the process of interaction of agents of cybersecurity systems in a simplified way.

3. The considered models belong to any one class (agent, system-dynamic, game, discrete-event), which predetermines the sets of simulated processes and objects.

The need to eliminate these shortcomings in modeling the processes of interaction of antagonistic agents in a cyber conflict, the systems of processes implies the aim and objectives of its achievement.

## 3. The aim and objectives of the study

The aim of the study is to develop a methodology for modeling the interaction of antagonistic agents in cybersecurity systems in a cyber conflict, based on the integration of various modeling methods.

To achieve the goal, the following objectives were set:

– to form a set of target models of the components of the process of interaction of antagonistic agents, describing the situation of cyber conflict and its dynamics;

– to develop a recursive agent model that implements reflexive behavior in the process of cyber conflict;

– to develop an integrated model of the interaction of antagonistic agents in cybersecurity systems.

## 4. Set of target models

The analysis of the process of confrontation in cyber security systems makes it possible to identify the following main components of it (Fig. 1):

– participants of interaction (Fig. 1 shows two participants – a defender and an attacker);

– problem area (cyber security system), a fragment of which is used as an object of attack by one side and as a tool to protect the other;

– confrontation environment;

– language (or languages) of the attack description that participants use to describe the process of interaction;

– attack model.

For the cybersecurity system to function effectively, the listed components must be represented by models of the appropriate type, which will allow the use of simulation results to predict the behavior of the adversary and develop an

effective protection strategy. Existing approaches to modeling such diverse components are very different in the degree of formalization, since they were developed in disciplines characterized by different levels of formalization. In addition, these approaches are described in terms peculiar to these disciplines (sometimes difficult to reconcile), which makes it difficult even to pre-structure the results obtained.

Thus, the main reason for the lack of a general theory of the antagonistic interaction process is multidisciplinarity and the extraordinary breadth of this phenomenon.

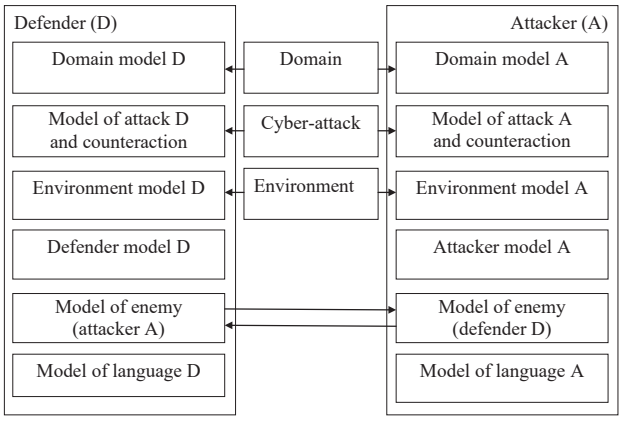


Fig. 1. Scheme of interrelation of models of components of antagonistic interaction

Let's note some differences of the proposed scheme of the interrelation of the components of the antagonistic interaction from similar schemes of the process of communicative communication. In general, the proposed scheme presents both software and hardware aspects of cybersecurity (attack, environment, problem area), and the socio-psychological characteristics of individuals involved in cyber conflict. First of all, it concerns the models of the attacker and the defender. The model of the person allows you to reflect the variety of roles that participants can perform in the conflict (in the first place, this concerns the attacker): from moral hackers to cyber-terrorists. The model of the enemy allows, within the framework of reflexive behavior and management, forming an image of the enemy and predicting his behavior and choosing means of counteraction corresponding to the incident based on the profile created. Similarly, an attacker, based on a reflexively constructed defender model, can form an attack scenario and correct it by evaluating the current behavior of the opposing party. Unlike similar schemes of classical communication processes, in a cyber conflict, opponents do not interact directly with each other. Therefore, they form a model of the enemy's behavior and correct the model of their own behavior only according to the manifestations of the cyber attacks being undertaken. The models mentioned allow the use of the entire mechanism of reflexive control, which currently didn't get the proper application in cybersecurity systems.

In the schemes of classical communicative communication, it is assumed that the interacting parties have or form a common language of communication, the use of which contributes to the achievement of a common goal. In cybersecurity systems, the goals of the conflicting parties are opposite, achieving a common goal or reconciling particular goals are out of the question. Therefore, in the proposed scheme, the language performs not so much an expressive function (the ability of the language to express and transmit information, affecting the interlocutor), as a gnoseological or accumulative function (the ability to reflect and store knowledge). The model of the attacker and defender language may not coincide, since there is no need to develop a common communication language.

The attack model, initially chosen by the attacker, can be fully formed, and for the defense side, it may not always be known while attacking, and can be completed or adapted during the attack. Similarly, we can talk about the model of countering the cyber attack.

Models of the presented components of the interaction of antagonistic agents of the cybersecurity system can be considered as elements of the situation arising in the process of cyber conflict. Combining various models as elements of a situation allows us to speak of modeling a situation as a set of events that develop in time and space and have certain consequences. This approach to modeling has its own characteristics and advantages over the standard approach to system modeling. The main property of the situation is its dynamism. The result is a consequence of the state and process, and external factors may influence the process. The principal difference between the methods of modeling situations is that it includes a process, that is, a dynamic element.

Therefore, the proposed methodology for modeling the interaction of antagonistic agents focuses on the use of an integrated situation model that combines particular models of both software, hardware and technology, and models related to the socio-psychological sphere of ensuring cybersecurity.

To implement the proposed idea, first of all, it is necessary to give a strict definition of the situation that will be used as a working one.

Let the initial state of the system be given, which is defined as follows:

$$W^0 = \left(M_D^0, M_A^0, M_M^0, M_1^0 ... M_n^0, M_L^0\right), \quad (1)$$

where (superscript indicates the initial state); $M_D$ – domain model; $M_A$ – attack model; $M_M$ – model of the environment in which cyber interaction occurs; $M_1$,..., $M_n$, – models of participants in cyber interaction; $M_L$ – language model.

Similarly, the target state of the system for the $i$-th participant can be defined.

$$W_i^F = \left(M_D^F, M_A^F, M_M^F, M_1^F ... M_n^F, M_L^F\right). \quad (2)$$

Let also the vector of resources be given that each of the participants in the interaction has at the initial moment of time:

$$R = \left(R_1, ..., R_n\right). \quad (3)$$

When time changes during the development of a situation as a result of the interaction of the system (problem area) and the environment, as well as the subsystems of the problem area, the system parameters change. The law of possible changes to the system parameters determines the vector of potential actions that, based on available resources and restrictions imposed by the environment and the subject area, the participants in the interaction can take, changing the state of the cybersecurity system:

$$A = \left(A_1, ..., A_n\right). \quad (4)$$

These actions can be considered as some operators that transfer the system from one state to another.

Then the vector:

$$Q = \left(W^0, A, W^F\right) \quad (5)$$

can be considered as a formal representation of the situation.

It is necessary to pay attention to the following. In the proposed interpretation, the state of the system and the situation developing in the system are not synonymous. The concept of a situation is much broader and includes the set *F*, defining the processes occurring in the system.

The presented situation definition is hierarchical. For example, the model of cyber attack can be represented as a set of phases, goals of each of them, the required resources at each phase, the duration of individual phases, up to individual elementary operations. The language reflected in the models can be fundamentally different in the initial and final states, which is illustrated by the model theory underlying the situational control. Another approach, namely, semiotic modeling, introduces algorithms of changes for all components used in defining formal systems.

Depending on the possible influences from the external environment and the opposite side, the following classes of situations are distinguished:

– simple situations where the initial state and possible outcomes have the composition and values specified a priori;

– complex situations in which the composition and values of the initial state and possible outcomes are a priori unknown;

– degenerate situations in which the initial state and possible outcomes can be represented by a linear combination of a priori known values.

Under the conditions of hybrid threats, it is impossible to predict many impacts on the system by the adversary and the cybersystem functioning environment, therefore the situations with which it is necessary to operate are initially complex. This means that it is not known in advance what types of cyber threats the information system may encounter during its operation.

The main property of the situation is its dynamism. The result is a consequence of the state and process, and external factors may influence the process. The principal difference of the situation is that its description includes a process, that is, a dynamic element. In the developed simulation model of the interaction of antagonistic agents, the main elements, presented in the formal definition of the situation, are implemented (section 6).

## 5. Recursive model of a reflexive agent

The combination (ideally integration) of a number of methods and models into a single whole to achieve a specific goal and methods for using them in the terminology of developing a cybersecurity system is a methodology. One of the purposes of the methodology is that it forces the developer to use a group of methods in a systematic way, providing a synergistic effect of modeling. Ideally, you need to have a complete set of methods integrated in some way to fully support the modeling process. A separate method that cannot be integrated with another is not only little practical, but it can also increase the risks of quality, productivity and complexity. Automating the implementation of integrated methods can be an ideal risk prevention strategy, but is not a requirement.

The methods used for modeling are necessary elements and are subject to analysis in the process of developing a methodology. The purpose of the methods is to reduce, first of all, the risks associated with a lack of information.

To achieve the goal of developing a methodology for integrated interdisciplinary modeling of cybersecurity systems, research and establishment of fundamental interrelations between various management tasks, concepts and tools to solve them are necessary. The ultimate goal of the development of a modeling methodology is to build a set of models reflecting various aspects and dynamics of the interaction process of antagonistic agents in cybersecurity systems that are included in the concept of the situation, as well as how to use them.

The basic principles of the proposed methodology for integrated modeling of the interaction of antagonistic agents of cybersecurity systems are taking into account the activity of individuals in the cybersecurity system (i.e., their own goals, interests, etc.), multimodality, integration and decentralization.

To implement these principles, we propose a methodology for constructing integrated complex models of situations arising in cybersecurity systems, the main elements of which are:

– multi-agent system as a conceptual carrier of the model, designed for conceptual, mathematical, and simulation modeling based on intelligent agents;

– multi-model complexes that allow the formulation, solution and receipt of calculation results for various classes of models included in an integrated situation model;

– integrated modeling system for connecting the planning and execution stages of work in the cybersecurity system, decision-making levels and the implementation of the «end-to-end» modeling principle «conceptual model – mathematical model – software product»;

– process of decentralized decision making in cyber security management.

In the proposed modeling methodology, active agents are considered not only from the point of view of computer modeling, but also from system-wide methodological positions as conceptual carriers of the model. This means that agents are not only a means of implementing software, but also act as elements of conceptual and mathematical modeling. This allows you to create a unified methodological basis for the analysis and modeling of cybersecurity systems with active elements.

An agent can be considered as an autonomous, problem solving and purposeful object with social abilities, capable of effective, proactive behavior. An agent can have his own goals, which he achieves by observing and acting in an open dynamic environment [40–42].

The agent is determined by a number of characteristics, the main of which include:

– attributes of the current state of the agent (information about its competencies and parameters of the process, for example, the current level of stocks, available resources, etc.);

– agent knowledge base;

– a set of incoming and outgoing messages (communication with other agents);

– selection function that determines the priority of incoming messages based on the knowledge base, current state and priorities (goals) of the agent.

Let's define a multi-agent system as consisting of a finite number of agents, actions, and situations. Denote by *N* the finite set of agents in the system. The final set of situations in which agents can function is denoted as *W*. It is assumed that each agent can perceive and recognize the situation. The

agent displays every possible perception on some real situation $w$; the set of all these situations is $W$. $A_i$, ($|A_i|>2$) denotes the final set of actions that an agent can take.

Agent $i$ perceives the state of the world $w$ and performs the action $a_i$ at each time step. It is assumed that the behavior of each agent can be described by a simple comparison of the situation with the action. It can also be assumed that there is a correct behavior for each agent. The target agent behavior consists of all the correct agent state and action mappings. To determine the target behavior for an agent, as a rule, for each $w \in W$ you need to know a set of actions that all other agents will perform in this situation $w$.

More formally, the behavior of each agent is represented by the decision making function $\delta_i : W \to A_i$ for agent $i$. This function maps each situation $w \in W$ to the action $a_i \in A_i$, that agent $i$ will take in this case.

The action that agent $i$ must perform in each situation $w$ (that is, the correct action for each situation $w$) is given by the objective function $\Delta_i : W \to A_i$, which also maps each situation $w \in W$ to the action $a_i \in A_i$. Since the choice of action for agent $i$ often depends on the actions of other agents, the objective function of agent $i$ must take these actions into account. That is, to generate a target function for $i$, you need to know $\delta_j(w)$ for all $j \in N_{-i}$ and $w \in W$. These functions $\delta_j(w)$ inform us about the actions that all other agents will perform in every situation $w$. You can use these actions with situation $w$ to determine the best action for agent $i$.

The measure of the correctness of the behavior of agent $i$ is estimated by an error, which is determined as follows:

$$e(\delta_i) = \sum_{w \in W} D(w) Pr\left[\delta_i(w) \neq \Delta_i(w)\right] = Pr_{w \in W}\left[\delta_i(w) \neq \Delta_i(w)\right],$$

where $D(w)$ is the fixed probability distribution of situations. The assumption of a fixed probability distribution makes it possible to estimate the probability that agent $i$ will take the wrong action. And this is the measure we use to evaluate how well agent $i$ works. Zero error means that the agent performs all the actions dictated to him by its target function. In the other extreme case (error is 1), the agent never takes actions dictated by its target function. All this forms the basis for the description of a multi-agent system.

The symbols used in the description of the work of agents are given in Table 1.

Inclusion of the decision-making agent model and the adversary model into the situation structure allows implementing the ideas of reflexive behavior and control with different levels of reflection. So an agent can be implemented as an instance of the simple decision function $\delta_i(w)$, or the agent can model the behavior of other agents using the decision function. Then use the predictions obtained by using these functions to determine what action to take. The agent can use an arbitrarily deep level of recursion of nested functions. In this case, they should be called $k$-level agents, where $k \geq 0$ and refers to the level of reflexivity that the agent uses.

Let's define an agent of the zero level as an agent who is not able to recognize the fact that in this situation other agents surround him. The zero level agent $i$ is implemented using a procedure that directly creates an instance of the decision function $\delta_i(w)$. This feature captures all the knowledge possessed by the agent.

The level 1 agent $i$ recognizes the fact that there are other agents in his environment and that they are taking actions, but he does not know anything about them. Given these facts, the strategy of the 1st level agent is to predict the actions of other agents based on their behavior patterns and to use these predictions when trying to determine own best action. The agent of the 1st level assumes that other agents choose their actions using the mapping $W$ to $A$. Therefore, the agent of the 1st level $i$ is implemented using procedures that directly create functions $\delta_i(w, \vec{a}_{-i})$ and $\delta_{ij}(w)$ for all agents. The behavior of the agent can be described by the function.

$$\delta_i(w) = \delta_i(w, \vec{a}_{-i}),$$

where

$$\vec{a}_{-i} = \left\{\delta_{ij}(w) \mid j \in N_{-i}\right\}.$$

In other words, the behavior of the agent of the 1st level can be described using the decision function, which is formed by the following composition of agent decision-making functions:

$$\delta_i(w) = \delta_i\left(w, \left\{\delta_{ij}(w) \mid j \in N_{-i}\right\}\right).$$

An example of an agent $i$ level 1, modeling two other agents $j$ and $k$, is presented in Fig. 3. Agent $i$ functions are presented, which include agent models $j$ ($\delta_{ij}$) and $k$ ($\delta_{ik}$). For example, $\delta_{ij}$ is a function that reflects the thoughts of agent $i$ that agent $j$ will do in every situation $w$. This action does not need to be performed by agent $j$, since model $j$ may be incorrect. That is, it is not necessary that the condition $\delta_{ij}(w) = \delta_j(w)$ be satisfied for all $w \in W$. When agent $i$ needs to determine what action to take, he first evaluates his models $j$ and $k$ to determine what actions he will perform ($a_j$ and $a_k$ in Fig. 2.). These actions then form a vector $\vec{a}_{-i} = \{a_j, a_k\}$. Since now there are values for $w$ and $\vec{a}_{-i}$, it is possible to evaluate the function for these values in order to obtain an action that agent $i$ takes, that is, $a_i$.

Table 1

Notation used to describe the behavior of agents in a multi-agent system

| | |
|---|---|
| $N$ | set of all agents, where $i \in N$ – one specific agent. |
| $W$ | set of possible situations, where $w \in W$ – one particular situation |
| $A_i$ | set of all actions that an agent can take. |
| $\delta_i : W \to A_i$ | agent $I$ decision function, determining the action of agent $i$, taken in each specific situation |
| $\Delta_i : W \to A_i$ | agent $I$ target function, indicating the action that agent $i$ should take. It takes into account the actions that other agents will take |
| $e(\delta_i) = \Pr\left[\delta_i(w) \neq \Delta_i(w) \mid w \in D\right]$ | agent $i$ error. This is the probability that agent $i$ will take the wrong action, given that a fixed set of situations $w$ is described by the probability distribution of their manifestation $D$ |

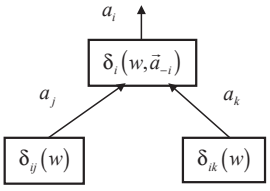


Fig. 2. Level 1 agent *i* determines what action to take

Similar to the presented implementation of reflexive agents, the level of nesting of models can be increased to the required value, which is dictated not so much by the complexity of the implementation of agents, as by common sense to the level of reflexivity of agents.

## 6. Integral model of interaction of antagonistic agents in cybersecurity systems

As an example, demonstrating the fundamental possibility of creating a reflective agent of a cybersecurity system, a model is presented in which the components of the confrontation process are modeled, namely, the defender, the attacker model and the environment model. These models have been implemented in the popular simulation environment PowerSim, which supports the principles of system dynamics. These models can be implemented within a separate agent to give it reflexivity properties.

The model focuses on the dynamics of the interaction of the attacker and the defender in the field of information security, which allows recognizing the strategies used by opponents.

The model represents a company in the form of a defender who secures information assets from a group of hackers (intruders) who are trying to violate the security of a company's assets with cyber attacks. An asset can take various forms: customer list, website, payables register or strategic plan. The level of security is determined by the degree of confidentiality, integrity, authenticity or availability of an asset for authorized users.

The model presents three possible threats that can be viewed as separate vectors of threats to the security of access to one of the company's assets. Each threat can be protected on the basis of the corresponding protection algorithm. For each security vector, there is one access method and one protection method. Finally, the defense is effective if it can compensate for incoming attacks.

The key exogenous and endogenous variables used in the model of the confrontation process are demonstrated in Table 2. One of the limitations of the model is the exclusion of the types of attacks and types of intruders from consideration.

Cyber attacks can come from the internal environment of the company or from the outside world. The model does not distinguish between internal and external intruders. Internal attackers include disgruntled employees and negligent employees who use weak passwords to access the system or follow the link from a fishing site. Another type of attacker is the external one, which generally includes hacker organizations of criminal activists. Instead, the attackers in this model are identical, and their number is not determined. In addition, the model does not break attacks into various types, such as denial of service, phishing, viruses, ransomware, and so on.

Table 2

The main indicators of confrontation

| Endogenous variables | Exogenous variables |
|---|---|
| Company reputation | Defenders capabilities |
| Successful attacks | Attackers capabilities |
| Vulnerability vectors | Attack unitary cost |
| Financial figures for defenders | |
| Malicious activity | |

The model does not reflect the financial aspects of ensuring cybersecurity, as this would require a more complex model, including empirical data, to give greater accuracy to research.

The structure of the model represents both the qualitative measurement of the system, through a causal relationship of variables, and its quantitative measurement, through the formal definition of these causal relationships in the form of equations.

As shown in Fig. 3, the system dynamics model contains three sub-models:

– a defender submodel;
– a battlefield submodel;
– an attacker submodel.

Fig. 3 shows a defender sub-model that represents the company's defense structure. In each period, the defender makes a decision about defining his defense configuration. Defenders are expected to have basic protection for each vector, and their security capabilities are designed to cover additional security efforts resulting from security breaches.

As shown in this figure, a defender protects his asset by manipulating three security vectors (A, B, and C). Ultimately, the success of the defense can be assessed by the degree of preservation or loss of the company's reputation.

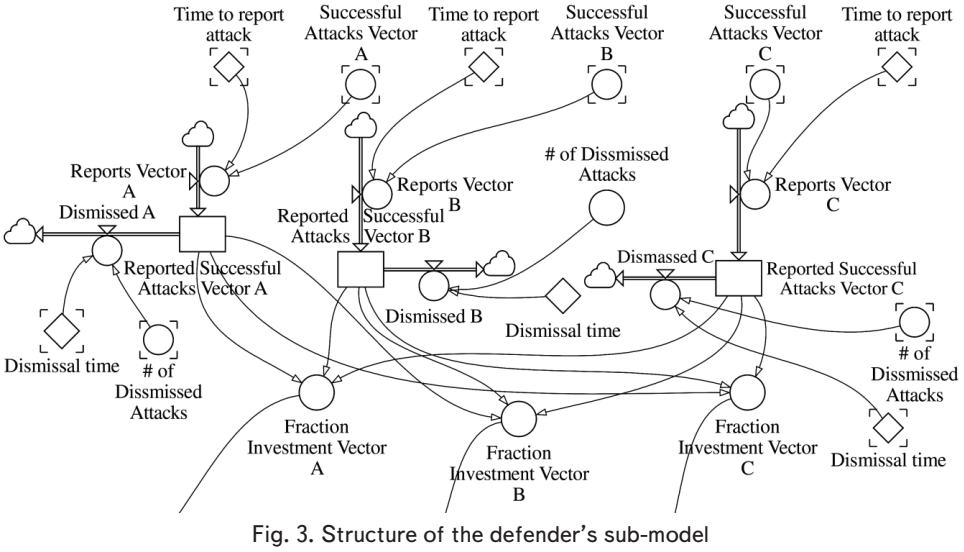


Fig. 3. Structure of the defender's sub-model

The submodel of the confrontation environment is a segment of the model in which defenders and intruders interact based on their own capabilities. The main components of this submodel are vulnerability and attack success for each security vector. Graphic representation of the submodel is presented in Fig. 4.

Vulnerability is determined by the difference between the resources that the attacker directs to the corresponding vector of attacks, and the resources that the defender allocates to eliminate security flaws within the same vector.

The attacker (Fig. 5) identifies and uses the «weak link» approach, that is, the security vector with the lowest protection. If the attacker succeeds, he will make a profit, which will mean lower financial performance for the defender. The attacker is valid only when it is economically feasible.

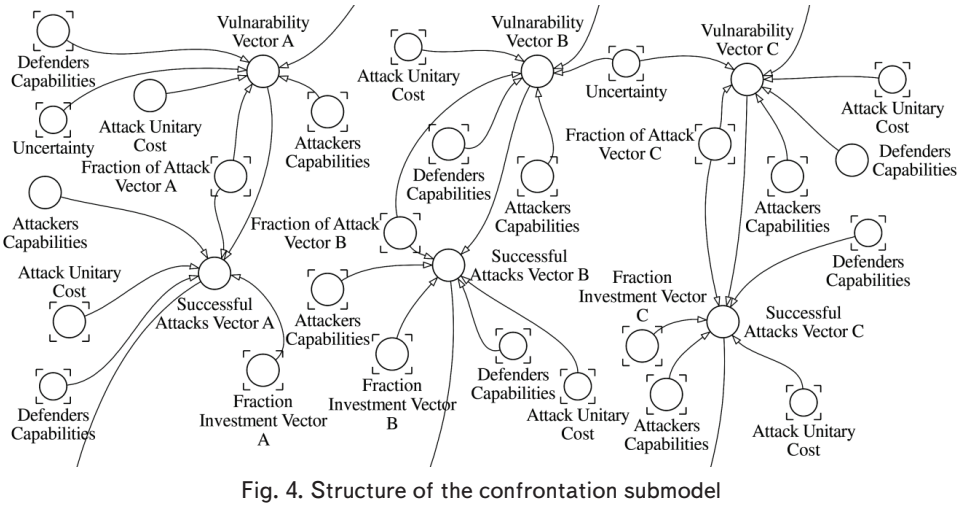


Fig. 4. Structure of the confrontation submodel

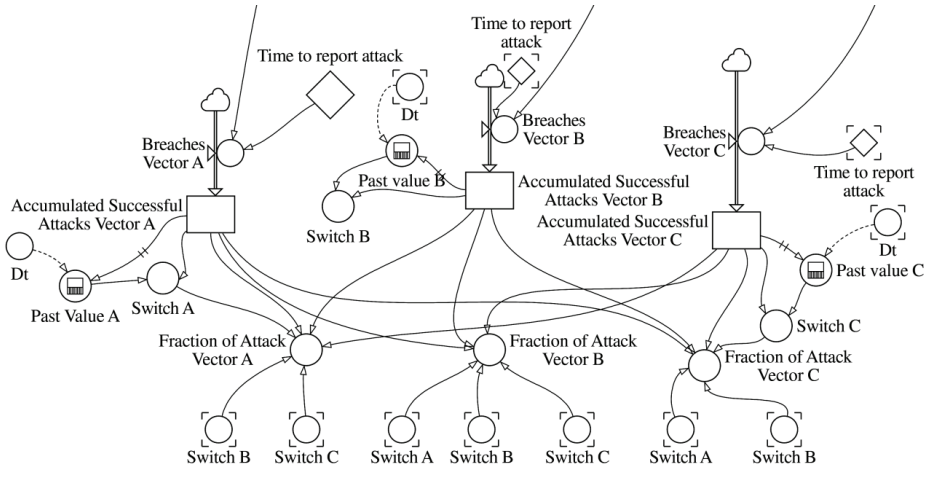


Fig. 5. Structure of the attacker's submodel

Successful attacks in an attacker model induce to attack the weakest link and not to neglect other vectors, allocating a smaller part of the resources for their attack.

The developed models are the basis for the creation of intelligent agents and multi-agent systems that implement the properties of reflexivity.

The use of a model not only of one's own behavior, but also of one's behavior with the ability to predict the consequences of such a choice, greatly increases the power of cyber-defense tools.

## 7. Discussion of the results of the development of methodology for modeling antagonistic agents in cyber security

In the course of solving the tasks posed to develop a methodology for modeling antagonistic agents in cybersecurity systems, the following results were obtained.

A set of target models of the components of the antagonistic agent interaction process were formed. This set includes the models of the attacker, the defender, the confrontation environment and the subject area of the considered processes, the attack model and the description language of the modeled processes. When implementing these models, emphasis was placed primarily on modeling the behavioral characteristics of cyber conflicts. This follows from the increasing role of a participant in a cyber conflict in the context of hybrid threats, when it is impossible not only to give a formal description of the behavior of the parties to the conflict, but also to predict in advance what type of attack will be received and what scenario of the conflict will develop. The advantage of this approach is the inclusion of elements reflecting all aspects of cyber conflict, both software and technological, and behavioral, in contrast to the previously proposed approaches that affect only one of the parties to the conflict.

It was proposed to consider target models as elements of a conflict situation, and model the development of cyber conflict to be implemented as a situation modeling. To support such an approach, a formal definition of the situation was given, including a variety of models, resources and possible actions of the opposing parties, which is significantly different from using the concept of the situation in management without using any formalisms. The advantage of the proposed approach is the possibility of transforming a formal description of a situation into a model.

The proposed approach, which is part of the modeling methodology, orients the cybersecurity expert to sharing the full variety of models, as opposed to independent modeling of individual components of confrontation processes in cyber conflicts. In contrast to the existing methods, the proposed method determines the coordinated use of various models, which makes it possible to improve the quality of modeling by compensating for the shortcomings of some models by the advantages of others. It is this feature of the proposed methodology that leads to a synergistic effect, both in the process of modeling and in the process of

using the results of modeling. Based on the need to model exactly the behavioral characteristics of all parties to the conflict, agent-based modeling was chosen as the conceptual basis of the modeling methodology. To develop the agent model, the main characteristics of the modeling methodology were determined, namely, the activity of interacting agents of the cybersecurity system (i. e., their own goals, interests, etc.), multi-model and integration (coordinated simultaneous use of models of various types) and decentralization (lack of a single decision-making center for all participants in a cyber conflict). These modeling characteristics were taken into account in the process of developing a formal description of an agent with elements of reflexive behavior. The proposed formalization includes a model of the agent's own behavior, a model of the probable behavior of the opposite side of the conflict, as well as a model for evaluating the effectiveness of the behavior of all parties to the conflict.

The agent model of an individual participant of the cyber-conflict was the basis for a simulation model of the interaction of antagonistic agents, including the submodels of the defender, the attacker, and the confrontation environment. The developed model can serve as a basis for modeling the reflexive mechanisms of formation of one's own behavior based on predicting the enemy's behavior and assessing the effectiveness of the actions of all parties to a conflict, taking into account the results of modeling the environment of their confrontation. In contrast to the existing models, the proposed model allows you to simulate the dynamics of all elements of a cyber conflict simultaneously. The developed model is adaptive, allowing not only parametric adaptation of individual variables (for example, resources of the conflicting parties), but also structural adaptation, manifested in setting behavior models for a specific type of attacks and countermeasures, which is necessary under conditions of hybrid threats.

As a general lack of research, the following should be noted. First of all, it is assumed that only two agents are involved in the cyber conflict, the defender and the attacker. In reality, this assumption may not always be adequate. For example, several attackers can be involved in a cyber attack, each of whom can implement their own cyber attack scenario. This may require a coordinated use of multiple countermeasures by the defending party. You can also note some «static» model in the sense that the model does not take into account the training of conflicting agents. These limitations of the developed model, which is the basis of the methodology, can be considered as areas for further research, during which both the types of models used and the corresponding modeling tools can be changed. In particular, learning mechanisms can be implemented using neural networks, maintaining the efficiency of agents may require the use of genetic algorithms, and data mining methods will allow for the implementation of situation recognition methods.

## 8. Conclusions

1. A set of target models of the components of the process of interaction of antagonistic agents has been formed, including the models of the attacker, the defender, the confrontation environment and the subject area of the processes under consideration, the attack model and the description language of the modeled processes. A formal definition of a cyber conflict situation is given, based on the use of a variety of models, resources and possible actions of opposing parties.

2. A recursive agent model has been developed, which includes the defender, attacker, and confrontation environment submodels. A distinctive feature of the model is the mechanism for implementing reflexive behavior and its adaptation to a given level of reflection.

3. An integrated model of the interaction of antagonistic agents in cybersecurity systems has been developed, including submodels of defender, attacker, and confrontation environment. The model supports simultaneous modeling of the dynamics of all parties to a cyber conflict, providing customization for a specific type of attacks, countermeasures and the level of available resources.

References


1. Evseev S. P., Koc G. P., Korol' O. G. Analysis of the legal framework for the information security management system of the NSMEP // Eastern-European Journal of Enterprise Technologies. 2015. Vol. 5, Issue 3 (77). P. 48–59. doi: https://doi.org/10.15587/1729-4061.2015.51468
2. Evseev S. P., Abdullaev V. G. Monitoring algorithm of two-factor authentication method based on passwindow system // Eastern-European Journal of Enterprise Technologies. 2015. Vol. 2, Issue 2 (74). P. 9–16. doi: https://doi.org/10.15587/1729-4061.2015.38779
3. Simulations in Cyber-Security: A Review of Cognitive Modeling of Network Attackers, Defenders, and Users / Veksler V. D., Buchler N., Hoffman B. E., Cassenti D. N., Sample C., Sugrim S. // Frontiers in Psychology. 2018. Vol. 9. doi: https://doi.org/10.3389/fpsyg.2018.00691
4. Gorodeckiy V. I., Kotenko I. V., Karsaev O. V. Mnogoagentnaya sistema zashchity informacii v komp'yuternyh setyah: mekhanizmy obucheniya i formirovaniya resheniy dlya obnaruzheniya vtorzheniy // Problemy informatizacii. 2000. Issue 2. P. 67–73.
5. Yevseiev S., Korol O., Kots H. Construction of hybrid security systems based on the crypto-code structures and flawed codes // Eastern-European Journal of Enterprise Technologies. 2017. Vol. 4, Issue 9. P. 4–21. doi: https://doi.org/10.15587/1729-4061.2017.108461
6. Kotenko I. V., Korsaev O. I. Ispol'zovanie mnogoagentnyh tekhnologiy dlya kompleksnoy zashchity informacionnyh resursov v komp'yuternyh setyah // Izvestiya Yuzhnogo federal'nogo universiteta. Tekhnicheskie nauki. 2001. Issue 4. P. 38–50.
7. Veksler V. D., Buchler N. Know your enemy: applying cognitive modeling in security domain. URL: https://pdfs.semanticscholar.org/7da6/5e3f224d4830bf0e7fdeae310fa4f52597ed.pdf
8. Cassenti D. N., Veksler V. D. Using Cognitive Modeling for Adaptive Automation Triggering // Advances in Intelligent Systems and Computing. 2018. P. 378–390. doi: https://doi.org/10.1007/978-3-319-60591-3_34
9. Kelley T., Amon M. J., Bertenthal B. I. Statistical Models for Predicting Threat Detection From Human Behavior // Frontiers in Psychology. 2018. Vol. 9. doi: https://doi.org/10.3389/fpsyg.2018.00466
10. Formalized Conflicts Detection Based on the Analysis of Multiple Emails: An Approach Combining Statistics and Ontologies / Zakaria C., Curé O., Salzano G., Smaïli K. // On the Move to Meaningful Internet Systems: OTM 2009. 2009. P. 94–111. doi: https://doi.org/10.1007/978-3-642-05148-7_9
11. Mitnick K. D., Simon W. L. The Art of Deception: Controlling the Human Element of Security. John Wiley & Sons, 2002. 368 p.
12. Whitman M. E., Mattord H. J. Principles of Information Security. Boston, MA: Course Technology, 2007.

13. Von Solms R., van Niekerk J. From information security to cyber security // Computers & Security. 2013. Vol. 38. P. 97–102. doi: https://doi.org/10.1016/j.cose.2013.04.004
14. Jones A., Colwill C. Dealing with the malicious insider // Australian Information Security Management Conference. 2008.
15. Colwill C. Human factors in information security: The insider threat – Who can you trust these days? // Information Security Technical Report. 2009. Vol. 14, Issue 4. P. 186–196. doi: https://doi.org/10.1016/j.istr.2010.04.004
16. Kraemer S., Carayon P., Clem J. Human and organizational factors in computer and information security: Pathways to vulnerabilities // Computers & Security. 2009. Vol. 28, Issue 7. P. 509–520. doi: https://doi.org/10.1016/j.cose.2009.04.006
17. Bowen B. M., Devarajan R., Stolfo S. Measuring the human factor of cyber security // 2011 IEEE International Conference on Technologies for Homeland Security (HST). 2011. doi: https://doi.org/10.1109/ths.2011.6107876
18. Alpcan T., Bazar T. Network Security: A Decision and Game-Theoretic Approach. Cambridge University Press, 2010. doi: https://doi.org/10.1017/cbo9780511760778
19. A Survey of Game Theory as Applied to Network Security / Roy S., Ellis C., Shiva S., Dasgupta D., Shandilya V., Wu Q. // 2010 43rd Hawaii International Conference on System Sciences. 2010. doi: https://doi.org/10.1109/hicss.2010.35
20. Something Smells Phishy: Exploring Definitions, Consequences, and Reactions to Phishing / Kelley C. M., Hong K. W., Mayhorn C. B., Murphy-Hill E. // Proceedings of the Human Factors and Ergonomics Society Annual Meeting. 2012. Vol. 56, Issue 1. P. 2108–2112. doi: https://doi.org/10.1177/1071181312561447
21. Keeping Up With The Joneses / Hong K. W., Kelley C. M., Tembe R., Murphy-Hill E., Mayhorn C. B. // Proceedings of the Human Factors and Ergonomics Society Annual Meeting. 2013. Vol. 57, Issue 1. P. 1012–1016. doi: https://doi.org/10.1177/1541931213571226
22. Aggarwal P., Gonzalez C., Dutt V. Cyber-Security: Role of Deception in Cyber-Attack Detection // Advances in Intelligent Systems and Computing. 2016. P. 85–96. doi: https://doi.org/10.1007/978-3-319-41932-9_8
23. Cyber Situational Awareness / S. Jajodia, P. Liu, V. Swarup, C. Wang (Eds.). Springer, 2010. doi: https://doi.org/10.1007/978-1-4419-0140-8
24. Dutt V., Ahn Y.-S., Gonzalez C. Cyber Situation Awareness // Human Factors: The Journal of the Human Factors and Ergonomics Society. 2013. Vol. 55, Issue 3. P. 605–618. doi: https://doi.org/10.1177/0018720812464045
25. Effects of Cyber Disruption in a Distributed Team Decision Making Task / Finomore V., Sitz A., Blair E., Rahill K., Champion M., Funke G. et. al. // Proceedings of the Human Factors and Ergonomics Society Annual Meeting. 2013. Vol. 57, Issue 1. P. 394–398. doi: https://doi.org/10.1177/1541931213571085
26. Achieving Cyber Defense Situational Awareness: A Cognitive Task Analysis of Information Assurance Analysts / D'Amico A., Whitley K., Tesone D., O'Brien B., Roth E. // Proceedings of the Human Factors and Ergonomics Society Annual Meeting. 2005. Vol. 49, Issue 3. P. 229–233. doi: https://doi.org/10.1177/154193120504900304
27. Human Factors in Cyber Warfare / Knott B. A., Mancuso V. F., Bennett K., Finomore V., McNeese M., McKneely J. A., Beecher M. // Proceedings of the Human Factors and Ergonomics Society Annual Meeting. 2013. Vol. 57, Issue 1. P. 399–403. doi: https://doi.org/10.1177/1541931213571086
28. Augmenting Cyber Defender Performance and Workload through Sonified Displays / Mancuso V. F., Greenlee E. T., Funke G., Dukes A., Menke L., Brown R., Miller B. // Procedia Manufacturing. 2015. Vol. 3. P. 5214–5221. doi: https://doi.org/10.1016/j.promfg.2015.07.589
29. Rassel S. J., Norvig P. Artificial Intelligence. A Modern Approach. Pearson Education Inc., 2003. 1408 p.
30. Druzhinin V. V., Kontorov D. S., Kontorov M. D. Vvedenie v teoriyu konflikta. Moscow, 1989. 288 p.
31. Homer J., Oliva R. Maps and models in system dynamics: a response to Coyle // System Dynamics Review. 2001. Vol. 17, Issue 4. P. 347–355. doi: https://doi.org/10.1002/sdr.224
32. Sterman J. Business Dynamics. Systems Thinking and Modeling for a Complex World. Boston: McGraw Hill Higher Education, 2000.
33. Barlas Y. Formal aspects of model validity and validation in system dynamics // System Dynamics Review. 1996. Vol. 12, Issue 3. P. 183–210. doi: https://doi.org/10.1002/(sici)1099-1727(199623)12:3<183::aid-sdr103>3.3.co;2-w
34. Luna-Reyes L. F., Andersen D. L. Collecting and analyzing qualitative data for system dynamics: methods and models // System Dynamics Review. 2003. Vol. 19, Issue 4. P. 271–296. doi: https://doi.org/10.1002/sdr.280
35. De Gooyert V. Nothing so practical as a good theory; Five ways to use system dynamics for theoretical contributions // 34th International Conference of the System Dynamics Society. Delft, 2016. URL: https://www.systemdynamics.org/assets/conferences/2016/proceed/papers/P1209.pdf
36. Repenning N. P. A Simulation-Based Approach to Understanding the Dynamics of Innovation Implementation // Organization Science. 2002. Vol. 13, Issue 2. P. 109–127. doi: https://doi.org/10.1287/orsc.13.2.109.535
37. Gubko M. V. Upravlenie organizacionnymi sistemami s setevym vzaimodeystviem agentov. Chast' 1. Obzor teorii setevyh igr // Avtomatika i telemekhanika. 2004. Issue 8. P. 115–132.
38. Jackson M. O. The Stability and Efficiency of Economic and Social Networks // Advances in Economic Design. 2003. P. 319–361. doi: https://doi.org/10.1007/978-3-662-05611-0_19
39. Novikov D. A. Cognitive games: a linear step-function model // Problemy upravleniya. 2008. Issue 3. P. 14–22.
40. Wooldridge M. An Introduction to Multiagent Systems. John Wiley & Sons, 2002. 368 p.
41. Wooldridge M., Jennings N. R., Kinny D. The Gaia Methodology for Agent-Oriented Analysis and Design // Journal of Autonomous Agents and Multi-Agent Systems. 2000. Vol. 3, Issue 3. P. 285–312.
42. Wooldridge M., Jennings N. R. Intelligent agents: theory and practice // The Knowledge Engineering Review. 1995. Vol. 10, Issue 02. P. 115. doi: https://doi.org/10.1017/s0269888900008122