The rapid development of computer technology, the emergence of modern cyber threats with signs of hybridity and synergy put forward strict requirements for the economic component of national security and especially the processes of ensuring the economy cybersecurity. The cybersecurity industry is trying to meet today's requirements by introducing new and more advanced security technologies and methods, but it is believed that such a universal approach is not enough. The study is devoted to resolving the objective contradiction between the growing practical requirements for an appropriate level of cybersecurity of business process contours while increasing the number and technological complexity of cybersecurity threats. Also the fact that threats acquire hybrid features on the one hand, and imperfection, and sometimes the lack of methodology for modeling the behavior of interacting agents of security systems should be taken into account. However, this does not allow timely prediction of future actions of attackers, and as a result, determining the required level of investment in security, which will provide the required level of cybersecurity.

The paper proposes the Concept of modeling the behavior of interacting agents, the basis of which is a three-level structure of modeling the subjects and business processes of the contours of the organization and security system, based on modeling the behavior of antagonistic agents. The proposed methodology for modeling the behavior of interacting agents, which is based on the Concept of behavior of antagonistic agents, allows assessing and increasing the current level of security by reducing the number of hybrid threats by 1.76 times, which reduces losses by 1.65 times and increases the time for choosing threat counteraction means by reducing the time to identify threats online by 38 %

Keywords: cybersecurity, antagonistic agents, modeling methodology, reflexive agent, multiagent systems, business process contour

UDC 681.32:007.5
DOI: 10.15587/1729-4061.2020.218660

DEVELOPMENT OF THE SPACE-TIME STRUCTURE OF THE METHODOLOGY FOR MODELING THE BEHAVIOR OF ANTAGONISTIC AGENTS OF THE SECURITY SYSTEM

O. Milov
PhD, Professor
Department of Cyber Security and Information Technology
Simon Kuznets Kharkiv National University of Economics
Nauky ave., 9-A, Kharkiv, Ukraine, 61166
E-mail: Oleksandr.Milov@hneu.net
A. Hrebeniuk
PhD*
A. Nalyvaiko
PhD, Associate Professor
Center for Military and Strategic Studies**
E. Nyemkova
PhD, Associate Professor
Department of Information Technology Security***
I. Opirskyy
Doctor of Technical Sciences
Department of Information Security***
I. Pasko
PhD, Senior Research
Scientific-Research Center of Missile Troops and Artillery
Herasima Kondratieva str., 165, Sumy, Ukraine, 40021
Kh. Rzayev
PhD, Associate Professor
Department of Computer Technology and Programming
Azerbaijan State Oil and Industrial University
Azadlyg ave., 20, Baku, Azerbaijan, AZ1010
A. Salii
PhD, Associate Professor, Deputy Head of Institute
Institute of Aviation and Air Defense**
U. Synytsina
PhD*
O. Soloviova
PhD
Department of Information Technology
Ivan Kozhedub Kharkiv National Air Force University
Sumska ave., 77/79, Kharkiv, Ukraine, 61023
*Department of Economic and Information Security
Dnipropetrovsk State University of Internal Affairs
Gagarina ave., 26, Dnipro, Ukraine, 49005
**National Defence University of Ukraine named after Ivan Cherniakhovskyi
Povitroflotskyi ave., 28, Kyiv, Ukraine, 03049
***Lviv Polytechnic National University
S. Bandery str., 12, Lviv, Ukraine, 79013

Received date 22.10.2020
Accepted date 04.12.2020
Published date 25.12.2020

1. Introduction

As the world becomes more technological and dependent on computers to monitor vital functions or conduct business, the importance of ensuring the security of these systems is becoming critical in everyday life.

The most volatile aspect of a cyber attack is the attackers themselves. Modeling only a network can show its weak-

nesses and potential attacks that can be implemented. But this does not provide any information about what attacks can be carried out by attackers, based on their point of view. Because each person is individual, the process by which an attacker will attack the network will be different for each attacker. Understanding differences between attackers and their behavior can be used to analyze the consequences of attacks, and then for early detection and prediction.

By simulating cyber attacks, focusing on how a real cyber attacker will make decisions based on skills, rules, and knowledge, it is possible to synthesize data about an attacker's behavior that would otherwise be difficult to achieve. The combination of rule-based and knowledge-based attack generation provides reliable and diverse generations of attack trajectories, while providing realistic results because rules and knowledge are constantly coordinated with each other. This means that rules cannot be applied if knowledge is underdeveloped, and knowledge flexibility cannot be used if the rules are too limited. Applying this scheme to simulation allows a better understanding of how many different types of attackers affect by analyzing the types of attacks performed and being able to learn what the attacker needed to know to perform attacks. Finally, you should turn to potential end users trying to protect their networks from attacks that intrusion testers didn't think of, or other tools that don't have security tools. This provides a deeper understanding of how vulnerabilities are exploited and how they can affect the network before an attack can occur, and then something can be done about it. The cybersecurity industry is trying to meet today's requirements by introducing new and more advanced security technologies and methods. Modern methods of studying cyber threats are usually performed using static analysis of network and system vulnerabilities. But only a few address the most volatile and most important part of the problem – the attackers themselves. The human factor underlying cybersecurity provides a better understanding of this issue and highlights the behavior of individuals as a key factor of greatest concern. The human element at the heart of cybersecurity is what makes cyberspace a complex, adaptive system. A comprehensive, interdisciplinary, comprehensive approach that combines technical and behavioral elements is needed to increase cybersecurity. Therefore, the creation of a scientifically sound methodology for modeling the processes of agent behavior in security systems is an urgent scientific and applied problem of theoretical and practical significance.

2. Literature review and problem statement

In recent years, research has been conducted on the dynamics and implementation of cyber attacks to better analyze the impact of those attackers. Studies have been conducted on the use of network vulnerabilities to identify possible and realistic ways to attack [1–6]. Thus, [1] provides specific examples of large-scale cyber attacks. The paper [2] analyzes the trend of using third-party service providers to gain access to victim organizations. A new paradigm of attack graph analysis, which complements the traditional graph-centric representation based on graphs adjacency matrices, is presented in [3]. The work [4] is devoted to the issue of forecasting potential attacks on the basis of observed attacks. [5] gives an example of a Bayesian network based on the current model of the security graph. The variable-length Markov model, which captures the features of attack tracks, which allows predicting the probable subsequent actions in current attacks, is analyzed in [6]. It should be noted that the disadvantage of these works is that these methods take into account only vulnerabilities in the network, but do not reveal real differences between the types of attackers. In other works, this issue was considered by modeling the capabilities of opponents [7] or applying the methodology of game theory [8] to simulate the attacker and defender. None of these methods simulate an attacker based on the information that an attacker receives during an attack, although it plays an important role in making decisions about the attack. This concept is well implemented in agent modeling methods in the NeSSi2 (NeSSi – Network Security Simulator) [9] and in the attacker's behavior model in multistage attack scenario simulation (MASS – multistage attack scenario simulation) [10]. However, agent modeling techniques do not provide a structure in which an attacker obtains specific details about targets and can dynamically change targets and strategies during an attack. This type of knowledge-based design for attacker modeling makes it possible to flexibly describe cyber attacks, which allows modeling the proactive and reactive behavior of participants in cyber conflict.

In [10, 11], simulations were performed to analyze possible cyber attacks that may occur in the network. The paper focuses on modeling the behavior of a cyber attacker so that it is possible to flexibly describe many different types of attackers, while maintaining reasonable realism in the types of attacks that can be performed. Modeling attacker's decision-making processes in terms of reflexive control is more like how an attacker actually thinks. This allows understanding the features that different attackers have in the same network, or how one attacker can affect different types of networks. This flexibility can help to ease the skills and to reduce the time to perform this type of analysis. The main goal is to develop a structure for modeling the attacker's decision-making process, based on both deterministic factors, such as network and knowledge, as well as probabilistic factors. This structure takes into account randomness in the simulation. Although the goal is not to be able to comprehensively model each type of attacker's behavior, but to determine what exactly needs to be modeled to describe the attacker.

Cyber threat analytics is a relatively young industry and is diverse in the types of approaches used to perform predictive cyber attack analysis. These approaches consist of vulnerability assessment and mitigation, analytical approaches such as the use of attack graphs and game theory, and mathematical and simulation modeling of cyber attacks. Each approach has its advantages and disadvantages, and one approach is not necessarily better than another because of the complexity of predicting, primarily human behavior. Currently, mathematical models such as attack graphs, attack ontologies or simulation, game theory models, or multi-agent models are used to analyze the enemy.

The purpose of a network intrusion test is to identify potential vulnerabilities in a network accessible to a

potential attacker. Knowing the vulnerabilities of the network, the tester/attacker can use them to further penetrate the network for more information. The intrusion tester will use this information to detect more vulnerabilities until the attackers have exhausted all their options. To do this, a so-called attack graph is developed, which is a set of all possible ways that an attacker can follow in the network. This process has traditionally been performed manually by an attacker or a group of analysts and can be a grueling process. In [12], the process is formalized to automatically generate a comprehensive set of possible attack graphs for a given network. Attack graphs are generated using a description of the network and the attacker's knowledge of that network, followed by a description of a set of states that describe the actual attacks that may occur. In [12], a network of two hosts with an IDS (IDS – Intrusion detection system) and a firewall was modeled. The result was an attack graph of 5,948 nodes with 68,364 edges, which is extremely large for very few types of attacks and unrealistically small network. This method of analysis is not flexible, scalable or easy to use, which is necessary to successfully assess network weaknesses.

Given the size of the network, it should be noted that the number of possible ways of attack can be extremely large. In [13], two methods were proposed to determine which attack graphs are the most critical and which are the most effective. Automatic attack graph generation requires modeling of all possible types of attacks. The paper [13] considered only 4 possible types of attacks.

[14] describes the use of attack graphs to generate IDS alert templates to help predict future and ongoing attacks. Using these attack graphs and knowledge of the area of cyber attacks, the probability of achieving attack goals to predict future attacks can be estimated. This method requires that each attack graph be converted to a network, and a cybersecurity expert analyze it to determine the likelihood of a successful cyber attack. This approach has two problems: the first attacks that do not strictly follow the attack plan cannot be modeled, and the probability is based solely on the expert's experience. [13, 14] define only the different ways that an attacker can follow, and not whether the attacker will actually implement this attack or not.

In [15], the authors eliminated the uncertainty of attack variation, success and accuracy of sensory warning data by combining attack graphs with Bayesian networks. This has led to the creation of real vulnerability databases, such as the National Vulnerability Database (NVD) and the Common Vulnerability Scoring System (CVSS). Using real data from these databases provides a basis for calculating the probability without the need for expertise for each function.

In [16, 17], the generation of a real-time attack graph is estimated to predict the probability of an attacker's next steps based on various security breaches. Based on security breaches, the basic level of attacker's skills can be determined, which can then be used with CVSS to determine the possibility of further steps based on the attacker's position in the network. A common problem of the above works is the development of a base attack graph that describes the attacker's scenario and targets. Using common attack pattern enumeration and classification (CAPEC) from MITRE, attack graphs based on real scenarios are generated in [18, 19]. These scenarios are used to obtain more realistic predictions and other attack graphs.

In [12–19], network security is analyzed on the basis of possible attacks that can be implemented in the network in one or more scenarios. In these cases, the scenarios are clearly defined, and different attackers may pursue the same goal, regardless of whether they are successful or not. Understanding the attacker's impact on a network is very important, because in fact not all vulnerabilities can be closed, and some can prioritize which vulnerabilities need to be addressed over time. Suppose there is an exploit that can be performed by anyone and that can have a harmful effect on the network. In this case, it should have a higher priority than the exploit, which only 1 % of attackers can perform on a non-critical machine. Publications [15, 17–19] show the use of publicly available data from cyber attack scenarios to create attack paths that were identified as realistic but did not take into account the skills or behavior of the attacker. Modern cyber attack predicting methods have become more focused on the behavior and decision-making of the attacker during the attack. Publications in scientific periodicals can be divided into two categories. The first category includes publications focused on methods of modeling the behavior of interacting agents. The second includes publications, focused on the behavioral aspects of security agents, and more specifically on decision-making processes. Attention to the use of game theory is due to the fact that this theory is the basis for agent modeling in conflict. Fig. 1 demonstrates the results of the analysis of modern approaches to agent behavior modeling, the main advantages of which are the following:

– reflection of the purposefulness of agents' behavior, as well as the agents' ability to formulate their goals in the model;

– ability to simulate both the behavior of an individual agent and the interaction between different agents that make up the model;

– learning ability of agents.

In [22–24], the authors propose approaches to assess the quality of service based on multifactor analysis and the current state of information security of the organization. However, possible preventive actions based on modeling and evaluating the capabilities of both the attacker and the defense side are not taken into account.

Thus, the analysis of the possibilities of ensuring both the security of the business process contour and the tasks of modeling the behavior of antagonistic agents, showed the following. Along with a large number of works on the security of organization's business processes, the problem of creating a holistic modeling methodology remains unresolved. The implementation of such a methodology in practice will contribute to the sustainable development of security systems of any level, based on modeling the behavioral characteristics of security system agents.

The lack of an appropriate methodology today is due to the contradiction, which is defined as follows. Practice requires the theory to find new approaches to cybersecurity and information security of the business process contour in terms of increasing the number of threats while increasing their technological complexity.

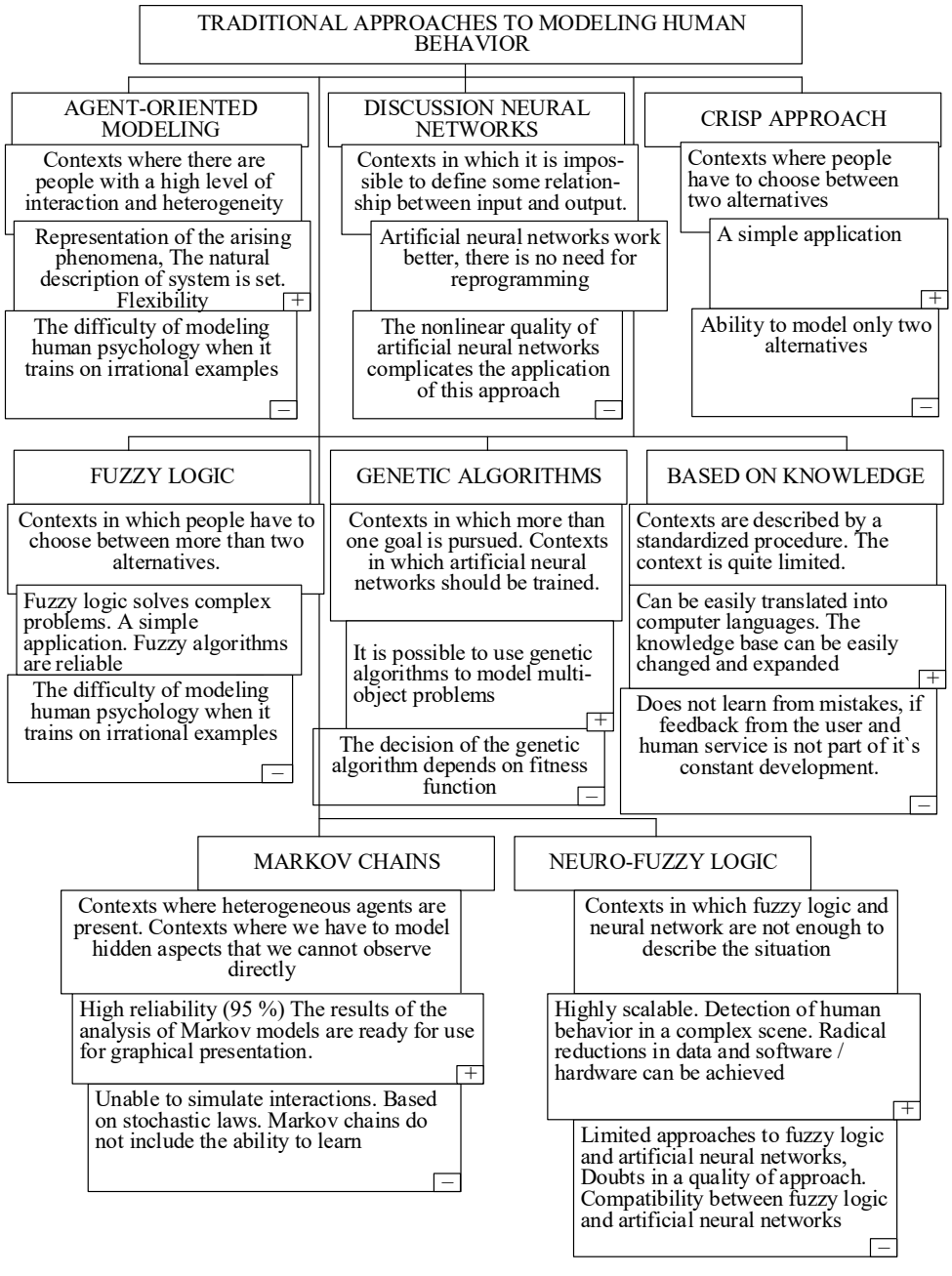

Fig. 1. Traditional approaches to modeling human behavior

3. The aim and objectives of the study

The aim of the work is to develop a space-time structure of the methodology for modeling the behavior of antagonistic agents of the security system based on the proposed models, methods and algorithms to determine the critical point of effective investment in security, to effectively resist modern hybrid threats to the elements of the business process contour structure, to increase the organization security level through an effective level of investment in the security system.

To achieve the aim, the following objectives are set:

– to identify the features of modeling the behavior of interacting agents of security systems in cyberconflict;

– to develop a concept for modeling the behavior of interacting agents;

– to develop a space-time structure of the methodology for modeling the behavior of interacting agents;

– to verify the proposed methodology by simulation.

4. Identifying the features of modeling the behavior of interacting agents of security systems in cyberconflict

When developing programs to simulate agent behavior, it is necessary to answer the question of how to model the decision-making processes of agents in the security system.

In computational social science in general and in the field of agent-based social modeling (ABSM), in particular, there is a constant discussion about the best way to simulate human decision-making. The reason for this is that most computational models of the decision-making process are

quite simple [25]. As with any good scientific model, when modeling human behavior, the objects being modeled should be analyzed in terms of only those properties that are relevant to the given behavior scenario.

Therefore, the question arises: "What is a good (computational) human (and decision-making) model for a particular research issue?" A large number of architectures and models have been developed for ABSM that attempt to represent the human decision-making process. Despite the common goal, each architecture has slightly different goals and, as a result, includes different assumptions and simplifications. Therefore, knowledge of these differences is important when choosing an agent's decision model in ABSM.

To be able to discuss the suitability of different agent architectures for different types of ABSM, it is necessary to answer the questions of which types of ABSM exist and which ones are of interest to the ABSM community.

One of the previous attempts to classify ABSM was made in [26]. The paper identifies five high-level aspects by which ABSM as a whole can be classified, including the extent to which ABSM attempts to include details of specific objectives. The last of these measurements concerns agents (and decision making), comparing ABSM by the complexity of the agents they model. According to Gilbert, this complexity of agents can vary from "product system architectures" (i.e. agents that follow simple IF-THEN rules) to agents with complex cognitive architectures such as SOAR (Security Orchestration, Automation and Response (symbolic cognitive architecture)) or ACT-R (Adaptive Control of Thought – Rational). Considering the suitability of different architectures for different research issues, [27] concludes that simpler agent models come in handy when the goal is to predict the behavior of the organization as a whole. Whereas accurate representations require complex and more cognitively accurate architectures to predict behavior at the level of individuals or small groups.

In [28], three categories of models are proposed:

– physical models that assume that people respond mutually to current (and/or past) interactions;

– economic models that assume that people respond to their future expectations and make decisions in a selfish way;

– sociological models that assume that people respond to their own and others' expectations (as well as to their past experiences).

In the classification [28], simple agent architectures, such as rule-based production systems, are best suited for physical models, and the complexity and capabilities of agents will need to increase in the transition to sociological models. In these sociological models, the emphasis on modeling social (human) interaction may require the agent to perceive the social network he or she is embedded in, or even the requirements for more complex social concepts.

Summing up, two main dimensions should be identified that are useful for distinguishing between agent architectures:

– cognitive level of agents, i.e. they are purely reactive or inspired psychologically or neurologically (to model person's decision-making as accurately as possible);

– social level of agents, i.e. the degree to which they are able to distinguish between social network relationships (and status), what levels of communication they are capable of, whether they have a theory of thinking or to what extent they are able to perceive complex social concepts.

Another way to classify ABSM in terms of applications is given in [29]. Examples of application areas include: emergence and collective behavior, development, learning, norms, markets, institutional design and (social) networks.

Other candidates for distinguishing agent architectures are:

– agents' ability to think about (social) norms, institutions and organizational structures; what impact norms, policies, institutions and organizational structures have on system performance at the macro level; and how to design regulatory structures that support the goals of the system developer (or other stakeholders);

– agents' ability to learn and, if so, at what level they can learn; for example, whether agents are able to learn only the best values of their decision-making functions and whether they can learn new decision-making rules.

So, two more dimensions should be added: norm and learning.

The last dimension proposed by researchers is the affective level that the agent is able to express. Most of the categories found are similar [29]. They also include emotions as an area of research.

Summing up, five main dimensions can be identified to classify the operation of ABSM in general and, therefore, to determine the agents architecture, which are shown in Fig. 2.

Fig. 3 shows the basic ABSM architectures, relevant models and application levels.

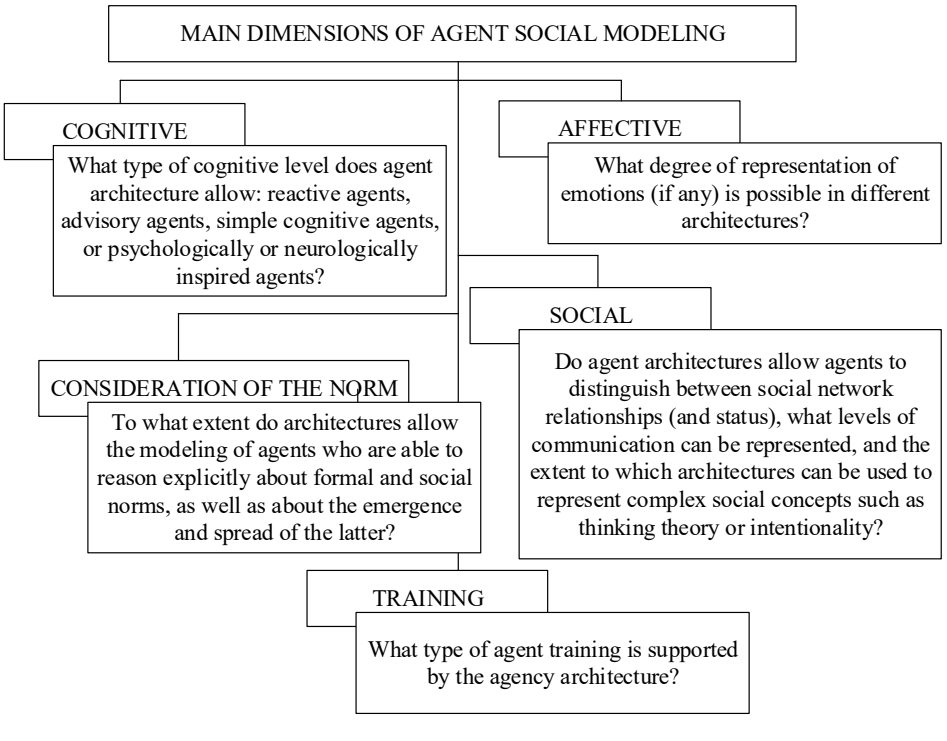

Fig. 2. Main dimensions of ABSM classification

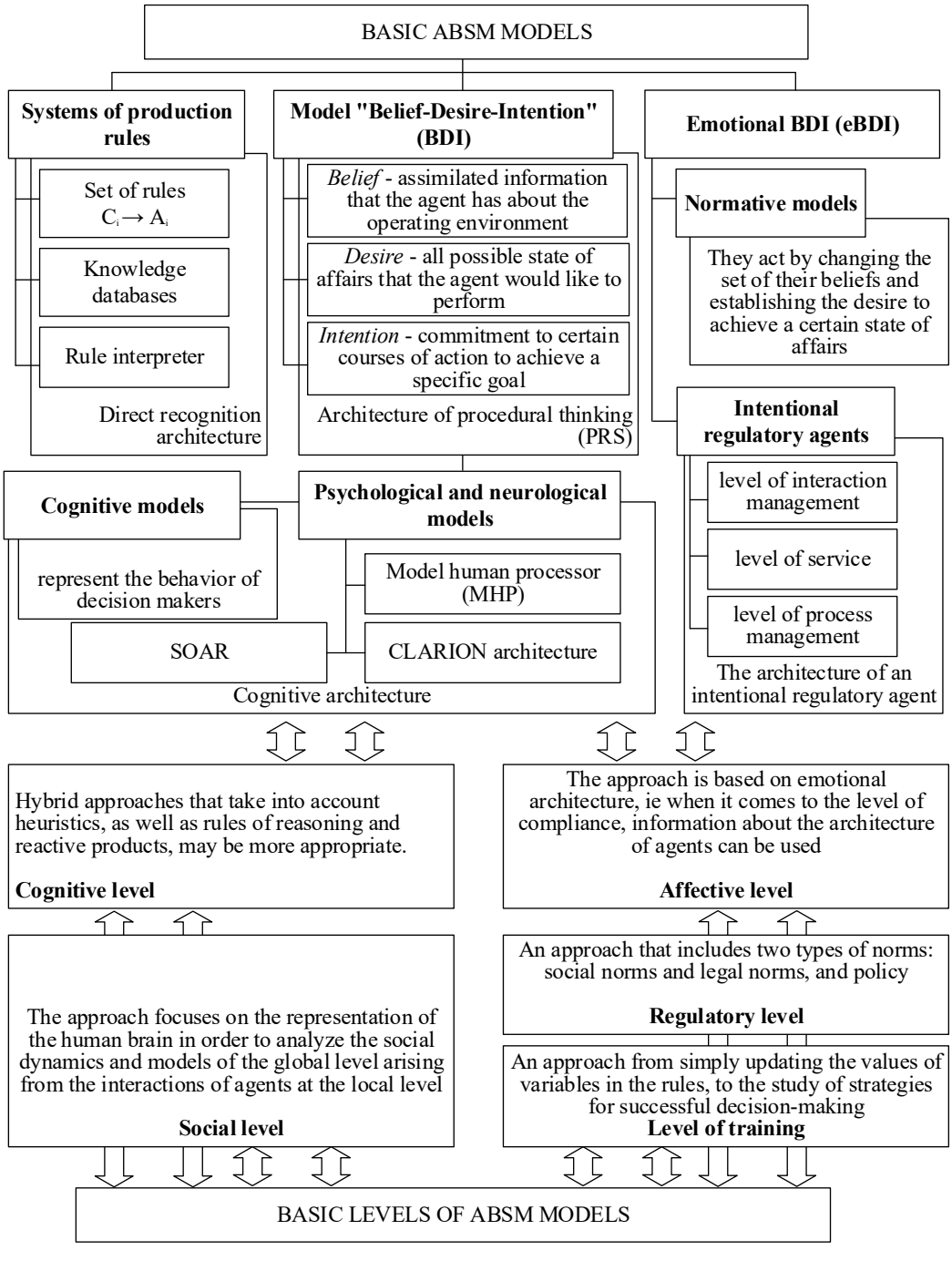

Fig. 3. Basic ABSM architectures, relevant models and application levels

Production rule systems are symbolic systems [31], which consist of a set of behavioral "IF-THEN rules" [30], and are an information processing architecture based on pattern matching.

The main components that make up production rule systems and determine which actions are selected by the agent on the basis of input data (the so-called direct recognition cycle [32]) are shown in Fig. 3.

Advantages:

– simplicity in terms of understanding the relationship between rules and their results;

– availability of convenient graphical tools for presenting decision-making processes (for example, decision trees).

Disadvantages:

– incomplete adequacy for modeling human behavior;

– agents of production rule systems are generally incapable of affective behavior, understanding and responding to norms, considering social structures (including communication), or learning new rules or updating existing ones;

– ability to model the agent's behavior only due to the great complexity and use of many rules;

– increase the likelihood of conflicts between the rules as their number increases;

– long computing time under a large number of decision-making rules.

The Belief-Desire-Intention (BDI) and emotional BDI (eBDI) models are one of the most popular models for agent decision-making in the agent environment. The model is es-

pecially popular for building reasoning systems for complex problems in dynamic environments [34].

In contrast to the production rule system, the basic idea of BDI (Belief-Desire-Intention) is that agents' mental state is the basis for their reasoning. As the name implies, the BDI model is centered around three mental attitudes, namely beliefs, desires, and especially intentions [35, 36].

Table 1 shows the advantages and disadvantages of the BDI model depending on the purpose (modeling) [37–40].

Table1

Advantages and disadvantages of the BDI model depending on the purpose

Purpose of modeling	Importance of BDI	Advantages	Disadvantages
Forecasting	Average	Realism, adaptable to behavior at the micro level, possibly irrational individual cognition	Complexity, scalability Detailed data is required
Task execution	High	Correct level of human behavior abstraction Awareness, cooperation in mixed human-agent teams Modular, scalable, flexible design	More complex design, unusual paradigm
Training	High	Accurate realistic behavior for better immersion in the game Adaptability to a dynamic environment Descriptiveness	More complex design, unusual paradigm
Using game theory	Average	Plausible human behavior: immersion, challenge Quick solution in case of uncertainty and incomplete information Correct level of abstraction to display real player strategies	Scalability, performance More complex design compared to scenarios
Education	Average	Intuitive explanation of behavior using built-in concepts of psychology (B, D, I)	Unnecessary realism and complexity for non-essential agents
Evidence	Low	Realistic knowledge needed to prove micro-, macro-connections and complex socio-cognitive phenomena	Realism and complexity are not needed to prove a simpler hypothesis
Revelation	Low	Realistic detailed behavior model for detecting unintuitive effects and micro-, macro-connections in adaptive dynamic complex systems	More complex understanding and deduction More complex specification of decision rules

Normative models [41]. In BDI, agents act by changing a set of beliefs and establishing a desire to achieve a certain state of affairs (for which agents then choose specific intentions in the form of plans they want to carry out). Agents' behavior is driven solely by their intrinsic motivators, such as beliefs and desires. The advantage of normative models was the use of an additional element that influenced the agent's reasoning. Unlike beliefs and desires, this element was external to the agent, and it took into account the behavioral norms established in the environment in which the agent was. Therefore, such elements were considered as external motivators, and agents in the system were called agents regulated by the relevant norms.

Intentional normative agents focus on the idea that social norms should be involved in the agent's decision-making process [42]. That is, autonomous agents should be able to reason, communicate, and negotiate norms, including deciding whether to violate social norms if they are unfavorable to commercial agents.

The advantages of this model are:

– ability to represent social norms not just as constraints and external fixed rules in the agent architecture [43], but also as mental objects. These objects have their own mental representation and interact with other mental objects (i.e. beliefs and desires) and the agent's plans [44];

– allocation of separate levels of the agent architecture. The first level is the interaction management level, which controls the agent's interaction with other agents (through communication), as well as the overall environment. The second level is the information service level, which stores the agent's information about the environment (information about the world), about other agents and about the agent society as a whole. The third level includes the process management level, where information is processed and decisions are justified.

This allows, on the one hand, considering the relevant processes as relatively independent, and on the other – as different manifestations of one general process of agent behavior;

– ability to display semantic differences between different types of information (three levels of information: one object level and two metalevels). The object level includes information that the agent believes in. The first metalevel contains information on how to process input information based on its context. Meta-information determines how an agent's internal processes can be changed and under what circumstances.

The disadvantages are as follows:

– emergence of an additional level of complexity due to the fact that the norms learned by the agent can affect both the generation and the choice of intentions.

Cognitive models [45] and social modeling models, although they often pursue the same goal (represent the behavior of decision-makers), tend to have a different idea of what is a good model for human decision-making.

As a disadvantage, it is noted that social modeling researchers often focus only on agent models specially adapted to the task, which limits the realism and applicability of social modeling.

The advantages of this class of models are clearly manifested in the form of the results of cognitive processes, namely the construction of so-called cognitive maps:

– clarity of factors influencing the decision-making process;

– clarity of connections between factors (not only qualitative, but also quantitative);

– ability to conduct so-called cognitive modeling, changing the weight of a factor that affects the final decision.

Psychological and neurological models are often referred to as cognitive architectures. However, because they have a different focus than the "cognitive architectures" that were

mentioned, they are allocated to a separate group. The main difference and advantage is that their architectures take into account the expected structural properties of the human brain.

Model human processor (MHP) [46, 47] is based on the synthesis of cognitive science and human-computer interaction. The advantage of the Model Human Processor is that it includes detailed specifications of the duration of actions and cognitive processing and breaks down complex actions into detailed small steps that can be analyzed. This allows system developers to predict the time it takes for a person to complete a task, avoiding the need to experiment with the people involved.

The advantages of the CLARION [48] architecture are as follows:

– use of hybrid neural networks for modeling problems in cognitive and social psychology, as well as for implementing intelligent artificial intelligence systems. This makes it relatively easy to implement architectures of this class on any artificial neural network platforms;

– presence of a built-in motivational structure and metacognitive structures;

– presence of two dichotomies: explicit and implicit representation, focused on action rather than representation;

– combining training from top to bottom and from bottom to top;

– inclusion of a number of functional subsystems that significantly expand both the scope of the architecture and the set of processes to be modeled. The main of these subsystems are as follows. The action-oriented subsystem that controls all actions. The action base subsystem supports knowledge, both explicit and implicit. The motivational subsystem provides the main motivation for perception, action and cognition. The metacognitive subsystem dynamically monitors and manages the operations of all subsystems.

Thus, the CLARION architecture combines reactive procedures, general rules, training and decision-making to develop universal agents that learn under specific conditions and summarize the knowledge gained in different environments.

SOAR [49] is a symbolic cognitive architecture that implements decision-making as purposeful behavior, which includes searching in the problem space and studying the results.

The advantages of this architecture:

– consideration of decision-making processes as a combination of search in the problem space, and study of the obtained results (i.e. feedback systems);

– combination of results of studying human behavior (descriptive models) and results of artificial intelligence (prescriptive models);

– use of two memory types in the system architecture: symbolic long-term memory (production rules), and short-term (working) memory (graph structure to allow the representation of objects with properties and relationships);

– ability to apply the rules in parallel, extracting several pieces of knowledge simultaneously;

– availability of additional context-sensitive knowledge for the decision-making process;

– distribution of operators according to several rules, which allows flexible presentation of knowledge about operators, as well as constant updating of knowledge structures for operators, allowing to redefine operators if required by circumstances [50, 51].

These models can be used at different levels of application, as shown in Fig. 3. For a more detailed acquaintance with the application levels of the models, please refer to the links [52–55].

5. Development of the concept of modeling the interacting agents behavior

To predict the possible behavior of the attacker, justify the choice of countermeasures for cyber threats at the systemic level and calculate the required amount of investment in cybersecurity with an appropriate distribution of areas and time of investment, a concept of modeling the behavior of security agents is proposed, which is implemented at three levels (level of security system, level of individual agents, level of agents group) and is aimed at ensuring the security of organization's business processes, which allows creating a business process contour of the security system (Fig. 4).

The following notation was used to formally describe the model basis of the concept of modeling the behavior of security agents.

For the ontology model: C – set, the elements of which are called concepts; H^C – hierarchy of concepts; R – set, the elements of which are called relations; – function that correlates concepts not taxonomically; $dom: R \to C$ – function that specifies the subject area R, and $range(R): \prod_2(rel(R))$ sets its range.

For the decision-making and training model: w – specific situation; W – set of all possible situations; DM_i – decision made by the i-th agent.

For the self-organization model: Σ – system structure; Φ – system function; R_w – emergence relations; G – set of goals; A – adaptability relations; P – set of memory elements; Θ – set of time points.

The following definitions are determined:

– definition 1. Critical business processes – processes whose improper organization or non-compliance with the requirements for their implementation may pose an actual or potential threat to product quality and, consequently, to business efficiency;

– definition 2. Organization's business process contour – a set of information resources and related business processes, the implementation of which in a given sequence ensures the achievement of the organization's goal

$$S^{BC} = \left\{ \left\langle S^{BP_1}, IR^{BP_1}, T^{BP_1} \right\rangle, ..., \left\langle S^{BP_n}, IR^{BP_n}, T^{BP_n} \right\rangle \right\}, \quad (1)$$

where S^{BP} – business process contour as a set of business processes, each of which represents: S^{Bpi} – i-th business process, defined by the structure of the links of individual business operations performed in a certain sequence; IR^{BPi} – set of information resources of the i-th business process; T^{BPi} – set of threats affecting the i-th business process;

– definition 3. Business process contour of the security system – a set of business processes and the resources necessary for them, the implementation of which ensures the proper functioning of the organization's business process contour:

$$S^{BP} = \left\{ \left\langle S^{BP_1}, Rs^{BP_1}, T^{BP_1} \right\rangle, ..., \left\langle S^{BP_m}, Rs^{BP_m}, T^{BP_m} \right\rangle \right\}, \quad (2)$$

where S^{BP} – business process contour of the security system as a set of business processes, each of which represents: S^{BSi} – i-th business process, defined by the structure of the links of individual business operations performed in a certain sequence in the security system; IR^{BSi} – set of information resources protected by the i-th business process of the security system; T^{BSi} – set of threats, protection from which provides the i-th business process of the security system.

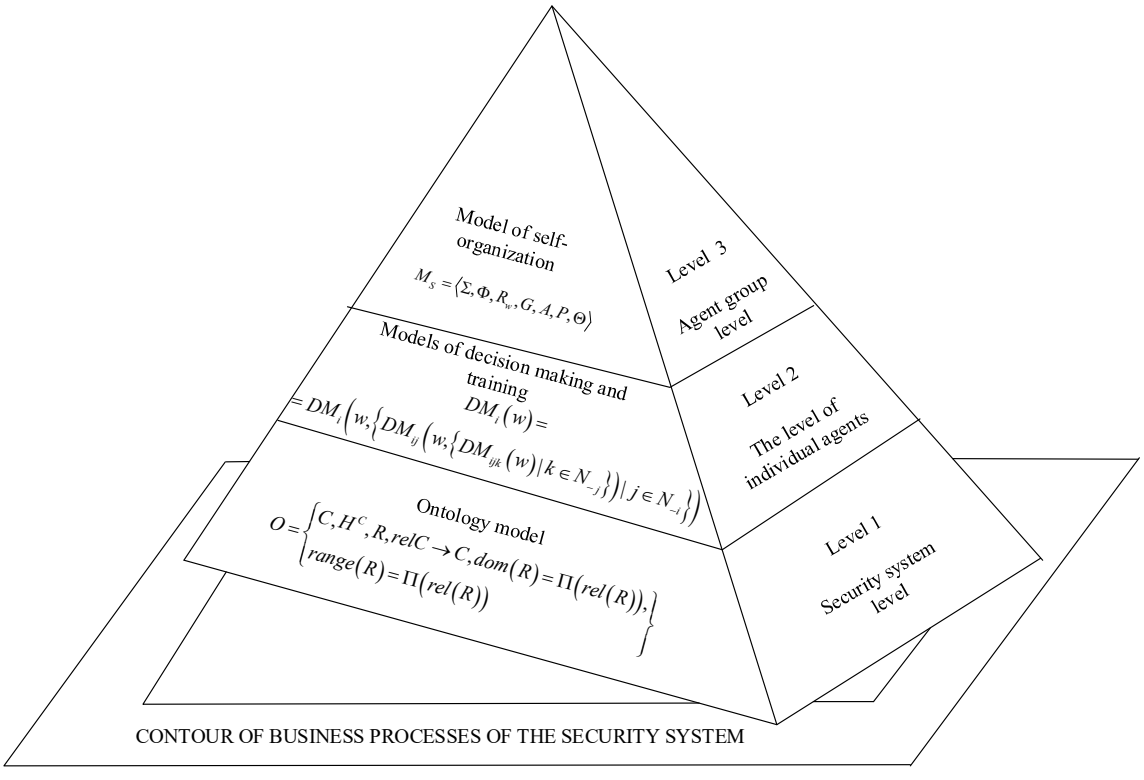

Fig. 4. Concept of modeling the behavior of security agents

The business process contour of the security system combines business processes: security management, security assurance, implementation, planning, testing and improvement.

At the first level of the Concept, the proposed ontological model is used as a carrier of knowledge about conflict-cooperative interactions of security system agents. The formalized ontology model is proposed as follows:

$$O = \begin{Bmatrix} C, H^C, R, relC \to C, dom(R) = \\ = \Pi(rel(R)), range(R) = \Pi(rel(R)) \end{Bmatrix}, \quad (3)$$

where C – set, the elements of which are called concepts; H^C:H^C – hierarchy of concepts, at $H^C \subseteq C \times C$; R – set, the elements of which are called relations, C and R do not intersect; $rel: R \to C \times C$ – function that correlates concepts not taxonomically; $dom: R \to C$ – function with $dom(R) := \prod_1(rel(R))$ sets the subject area R, and $R \to C$ with $range(R): \prod_2(rel(R))$ sets its range. For $rel(R) = (C_1, C_2)$, write down $R(C_1, C_2)$; A^O – set of ontology axioms, expressed in the corresponding logical language.

The analysis of the classifier of existing threats, which is proposed in [56], allowed us to formulate the relationship between hybridity and synergy of threats depending on their type and direction. The threat classifier introduces a platform of cost indicators of attacks, which allows assessing threats in terms of their economic efficiency and counteraction. The scale of measuring the cost of losses for expert evaluation is proposed in the form: {insignificant, low, medium, high, critical}. Let us mark: i – current threat number $\left(\{i\}_1^N\right)$, k – current number of the expert who performed the assessment $\left(\{k\}_1^K\right)$. The average experts' estimate of the cost of losses for all threats for a certain business process contour for defenders, and the cost of the whole set of attacks for attackers can be written as follows:

$$P_k^A = \frac{1}{KM}\sum_{j=1}^{M}\sum_{i=1}^{K}\alpha_j p_{ijk}^A; \; C_k^A = \frac{1}{KM}\sum_{j=1}^{M}\sum_{i=1}^{K}\alpha_j c_{ijk}^A, \quad (4)$$

$$P_k^D = \frac{1}{KM}\sum_{j=1}^{M}\sum_{i=1}^{K}\alpha_j p_{ijk}^D; \; C_k^D = \frac{1}{KM}\sum_{j=1}^{M}\sum_{i=1}^{K}\alpha_j c_{ijk}^D,$$

where K – number of experts, M – number of business operations that may be targeted by the threat, α_j – criticality ratio of the business process to which the relevant business operation belongs, p_{ijk} – assessment of the cost of losses from the i-th threat to the j-th business process by the k-th expert (the upper index identifies A – attacker, D – defender), c_{ijk} – similarly for the cost of implementing threats.

At the second level of the Concept, the issues of behavior of individual security system subjects are considered and models of their behavior are constructed, namely decision-making $\left(M_R^{DM}\right)$ and training models $\left(M_R^L\right)$: $M_R = \left\{M_R^{DM}, M_R^L\right\}$.

At the third level of the Concept, the previous level models are used to build group behavior models, namely coordination, adaptation and self-organization models: $M_G = \left\{M_G^C, M_G^A, M_G^{SO}\right\}$.

Thus, the concept of modeling the behavior of interacting agents is developed, the basis of which is a three-level structure of modeling subjects and business processes of the organization and security system contours. The proposed concept differs from the existing ones by using a synergistic threat model in the formation of areas for protecting information resources of the business process contour.

6. Development of space-time structure of the methodology for modeling the behavior of interacting agents

Based on the purpose of the methodology, it should reflect behavioral processes from two sides. On the one hand, display the processes related to the behavior and characteristics of an individual security agent. And on the other hand – the behaviors and processes that arise as a result of the joint functioning of agents. It is necessary to pay attention to modeling the environment of agents, because such an environment is a carrier of system-forming functions that significantly affect the behavior of a party to the conflict and their characteristics.

Within the framework of the proposed concept, a sequence of developing models, methods and algorithms that make it up is formed. The process of building the methodology consists of 5 stages.

Stage 1. Analysis of BP contours and possible attacks on them

$$S^{BC} = \left\{ \left\langle S^{BP_1}, IR^{BP_1}, Tr^{BP_1} \right\rangle, ..., \left\langle S^{BP_n}, IR^{BP_n}, Tr^{BP_n} \right\rangle \right\}, \quad (5)$$

where S^{BP} – business process contour as a set of business processes, each of which represents: S^{Bpi} – i-th business process given by the structure of the links of individual business operations performed in a certain sequence; IR^{BPi} – set of information resources of the i-th business process; T^{BPi} – set of threats affecting the i-th business process.

Stage 2. Development of models of the individual security system agent level

$$M_A = \left\{ M_A^{DM}, M_A^L \right\}, \quad (6)$$

where M_A – individual agent model; M_A^{DM} – agent's decision-making model; M_A^L – agent's training model.

Stage 3. Development of models of the security system agent group level

$$M_G = \left\{ M_R^B, M_R^L \right\},$$

where M_G – agent group model; M_R^B – agent group behavior model; M_R^L – agent group training model.

Stage 4. Development of models of the system-wide level

$$M_S = \left\{ M_S^C, M_S^{SO} \right\},$$

where M_S – system-wide level model; M_S^C – coordination models; M_S^{SO} – self-organization model.

Stage 5. Development of methods for determining the most likely threats and assessing their cost indicators

$$Tr_l = \arg \max_{\forall Tr_l \in Tr_C^D} K_l^D \cdot K_l^A, \quad (7)$$

where K_i^A – rating coefficient (importance) of implementing the threat to the i-th information resource; K_j^D – rating coefficient (importance) of building protection of the j-th information resource.

Below are the corresponding sets of models, methods and algorithms that form a particular level of methodology, with a brief description of the content of this level. It is clear that all the processes that take place in the business process contours, the security of which is provided by security agents, are significantly affected by threats aimed at disrupting the normal functioning of business processes. Threats are implemented through attacks on all components of security, namely, cybersecurity, information security and security of information. As a result, the analysis of business process contours as the main purpose of threats directed on it should begin with the analysis of threats, the set of which is reflected by the classifier with the relevant indicators. The compliance of the threat classifier with all models, methods and algorithms of the methodology determines and guarantees the effectiveness of the methodology for modeling the behavior of security agents in general. Thus, the analysis of the business process contour should begin with the analysis and improvement of the threat classifier. In addition to the existing platforms 1–4, a new platform has been added to the threat classifier – a platform of attack cost indicators. This allows assessing threats in terms of their economic efficiency and counteraction. The improved classifier of threats to the security of information resources, in contrast to the existing ones, contains cost indicators of threat implementation and counteraction. The improved classifier also allows assessing the likelihood of a threat and developing an effective defense strategy (Fig. 5).

Marks in Fig. 5 have the following meaning:

– for the ontology model: C – set, the elements of which are called concepts; H^C – hierarchy of concepts; R – set, the elements of which are called relations; $rel: R \to C \times C$ – function that correlates concepts not taxonomically; $dom: R \to C$ – function that specifies the subject area R, and $range(R): \prod_2(rel(R))$ sets its range;

– for the business process contour model, the labels were described earlier;

– for the threat classifier: i – current threat number $\left(\{i\}_1^N\right)$, k – current number of the expert who performed the assessment $\left(\{k\}_1^K\right)$;. P_k^A, C_k^A – average experts' estimates of the probability and cost of attacks for all threats; P_k^D, C_k^D – similar estimates for defenders; K – number of experts, M – number of business operations that may be targeted, α_φ – criticality ratio of the business process to which the relevant business operation belongs.

The resulting model of the first level of the methodology is a model of the ontology of relationships between the agents of the parties to the cyber conflict, which can be considered as a carrier of knowledge about the subject area. To build the model, the approach of automated ontology construction based on various scientific sources (planar texts) TextToOnto was used. The ontology model of agent behavior in the conflict conditions contains basic concepts of interaction processes of security system agents, and also concepts reflecting the interaction of counteraction agents, instead of technical parties of a cyber conflict. This orientation of the ontology model allows justifying the choice of a behavior model of antagonistic agents in the conditions of hybrid threats.

At the level of individual agents, the basic model is a model of a reflexive agent (Fig. 6). The main assumption of building a model is the assumption that the decision maker is considered as an information channel. In this case, the main indicators of its functioning can be obtained using information theory. These include bandwidth, generation, blocking and coordination of information. These indicators can be used for both an individual agent and a group of agents.

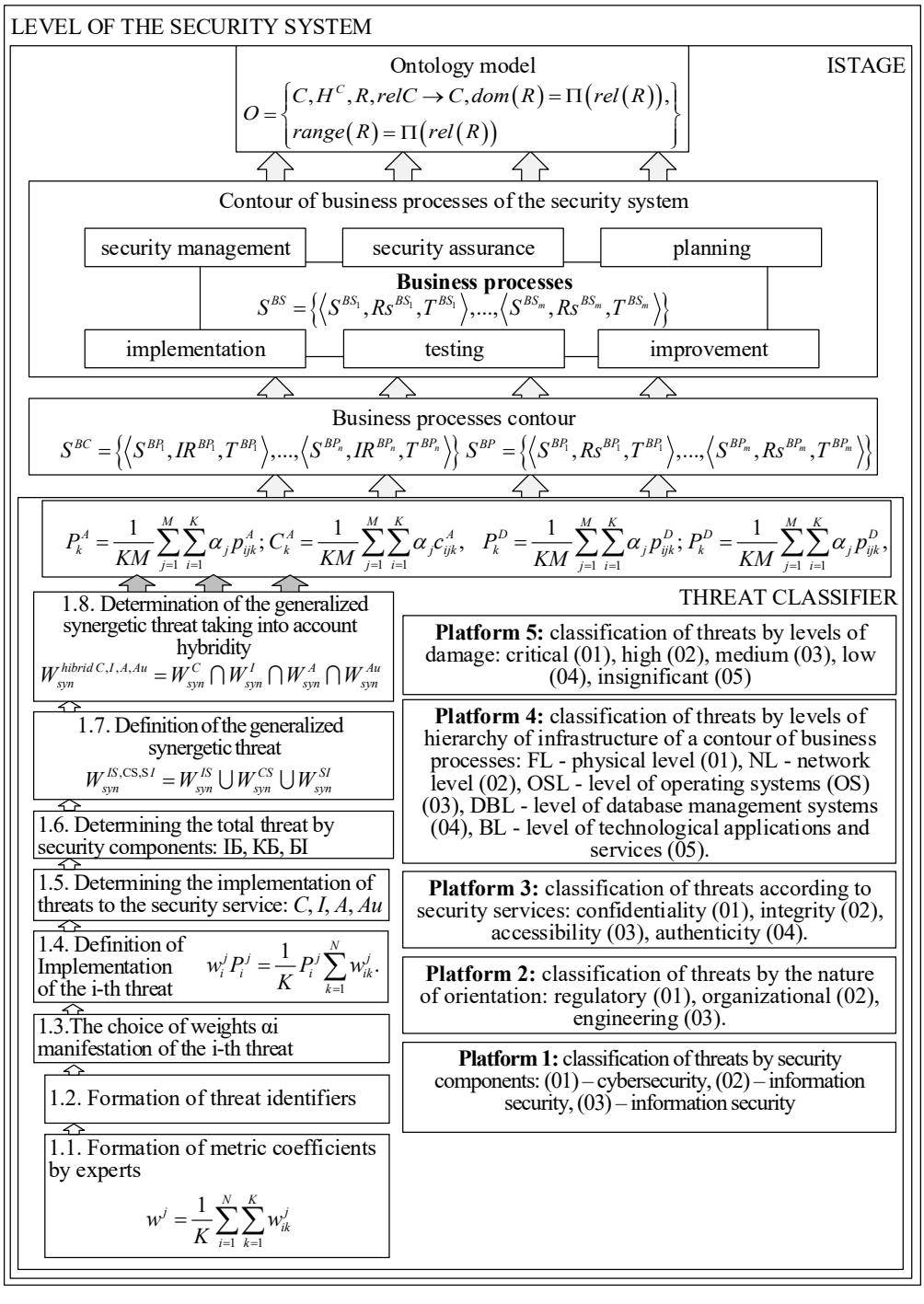

Fig. 5. Main components of the I stage of methodology construction (level of security system)

Fig. 6. Main components of the II stage of methodology construction (level of individual agents).

In Fig. 6, the following marks are used: w – specific situation; W – set of all possible situations; DM_i – decision made by the i-th agent; a_i – actions of the i-th agent; G_i – goals pursued by the i-th agent; $e(DMi)$ – agent's error when his decision does not meet his purpose; f_i – agent situation assessment function; cf – function of coordinating the decision of the i-th agent with the decision of other agents of the environment; h_i – threat counteraction selection function; ch – function of coordinating the choice with the choice of other agents.

The basic function of a security agent is the decision function. These decisions can concern both the process of assessing the situation and determining the type of threats, and determining countermeasures. The basic decision-making model proposed at this level by an individual agent implements the decision-making process in two stages. Each of these stages (assessment of the situation and choice of countermeasures) involves the coordination of the formed estimate with the estimates of other decision-makers. The presence of the processes of information exchange at all stages of decision-making with other cooperating agents in the dynamic behavior model of an individual agent, in contrast to existing models, is a significant difference. Taking into account this feature of decision-making behavior significantly affects the effectiveness of business process contour protection from cyber attacks in the

conditions of hybrid threats. Such an exchange can be considered as a basis for forming group behavior scenarios.

The second feature of the model is the ability to assign a level of reflection, which allows the counteraction party to build a model of possible behavior of the counteraction party to the conflict. Thus, a zero level of reflection indicates that the security agent has no information about the agent environment of counteraction. Whereas the first level of reflection indicates that the agent has an idea of functioning in the environment of other agents.The second level indicates that the opposite side of the conflict is also reflexive, i.e. has a model of behavior of the opposite side, and so on. The recursive model of the reflexive agent contains models of the attacker behavior and allows modeling the probable actions of attackers, and thus predicting the consequences of decisions made by the defense. Analysis of the reflexive abilities of agents shows that it is impractical to implement reflection above the 2nd level.

The second feature of the model of an individual security agent is the ability to take into account learning processes when countering cyber threats. The learning processes also reflect the reflexive properties of agents. In traditional learning models, it is possible to accumulate information about changes in the behavior of the opposite side of the conflict and to make predictions about the actions of the opposite side of the conflict. That is, one's own behavior is carried out within the framework of formal decision-making theory as a game against passive nature. And training in the face of the active side of the conflict takes into account that the enemy is an active agent, has its own goals and responds based on their own goals and taking into account the previous actions of the enemy. That is, the opposite side is active and also implements the learning process, i.e. the choice of reaction should be analyzed on the basis of game theory and taking into account the reflexive abilities of the agent.

Thus, at the level of individual agents, models of training of reflexive agents are proposed, which differ from traditional training models in that they take into account changes in the behavior of agents of the environment. To assess the quality of training and the dynamics of processes, the following indicators are proposed: the rate of changes in agent decisions, the rate of changes, the retention rate, and the generalized volatility ratio. The proposed coefficients show how long the agent will adhere to the decision, the agent's willingness to review the previous decision and his ability to respond quickly to changes in the environment of counteraction.

In contrast to the existing ones, the proposed model of agent training takes into account the multi-agent operating environment, which allows adapting agent behavior in a dynamic environment. In other words, when training, the agent takes into account the fact that he is in the process of counteraction with an active opponent. An active opponent may have his own goals, is characterized by an appropriate level of rationality, and has the ability to learn.

To develop models of the third level of methodology, the behavior model of an individual agent is modified to take into account the dynamics of processes and interactions of individual agents. That is, the agent's reaction is formed not only under the influence of the obtained results of the situation analysis, but also taking into account similar decisions made by agents of the dynamic environment (Fig. 7).

In Fig. 7, the following notation is used: $W=\{w_i\}$ – set of counteraction states (information about cyber attacks); $A=\{a_i\}$ – set of actions that an agent can perform; $Z=\{z_j\}$ – set of states in which the agent may be; $z_i(t+1)=f_i\left(z_i(t),u_i(t),w_i(t)\right)$ – transition function; $u_{ij}(t)=g_{ij}\left(z_i(t)\right)$ – aggregation function; $C=c_i\left(z_i(t),z_i(t+1),u_i(t),w_i(t)\right)$ – local cost function; $a_i(t)=h_i\left(z_i(t),u_{ji}(t)\right)$ – local output function.

The level of the agent group should include various methods of coordination in the groups of security agents. Different methods of coordinating agent behavior are explained by the fact that the method takes into account the level of agent reflexivity. Thus, the method of coordination without communication reflects the fact that the agent has the 0 th level of reflexivity, i.e. it is an agent that in no way takes into account the functioning of such agents. The method of coordination with abstraction, on the contrary, is used in the case when the agent builds a model of the opponent's behavior, which in turn also has a model of the opponent's behavior. The use of different methods of coordination allows organizing cooperation between security agents to ensure cybersecurity in a fairly wide range of operating conditions.

The application of the proposed characteristics to assess the effectiveness of the agent functioning can be demonstrated by the example of two structures of agent interaction. The first structure is parallel, when agents work together, possibly independently, coordinating their actions independently.

In the second structure, one of the agents coordinates the work of the other two agents. Knowledge of the specific characteristics of agents, in particular their effectiveness in making decisions and coordinating work, will allow concluding which of the structures is more effective in terms of productivity of a group of agents.

The method of assessing the effectiveness of the structure of interaction of a group of security agents allows justifying the choice of the interaction structure, as well as distributing the functions of protection of business process resources, which provides increased security of the business process contour. In contrast to the existing ones, the proposed method considers the agent as a processor of information with appropriate characteristics and is based on information processing processes and relevant characteristics of the effectiveness of the security system.

The final self-organization model combines models of the structure and functions of the security system, the relationship of emergence and adaptability, as well as sets of goals, memory elements, time points and input influences. The self-organization model provides the construction of a robust security system in the conditions of synergetic and hybrid threats, is based on the synergy of advanced models, and provides emergent properties of business processes in the security loop. The ability to aggregate models that focus on hybrid and synergistic threats significantly distinguishes it from known similar models (Fig. 8).

In Fig. 8, the following notation was used for the self-organization model: Σ–system structure; Φ – system function; R_w – emergence relations; G – set of goals; A – adaptive relations; P – set of memory elements; Θ – set of time points.

The main purpose of developing a methodology for modeling agent behavior is to increase the level of security of the organization's business process contour. This is done by obtaining an estimate of the likelihood of an attack on business processes and information resources

that ensure their functioning. The proposed algorithm for assessing the economic effectiveness of threats and countering them allows identifying the most likely threats aimed at violating the security of information resources. As a result, it is necessary to economically justify the distribution of limited funds between different information resources and business processes that require protection. The proposed algorithm for determining the most likely threat allows organizing an effective allocation of limited funds to protect the resources of the business process contour. This is done on the basis of using the results of modeling the behavior of cooperative-antagonistic agents, to determine and assess the likelihood of a threat. The model of determining the most probable threat allows organizing an effective allocation of limited funds to protect the resources of the business process contour based on the results of modeling the behavior of cooperative-antagonistic agents to determine and calculate the probability of threats. The proposed evaluation algorithm takes into account possible decisions on the attack and countering it, made by all parties to the cyber conflict in conditions of synergistic and hybrid threats. That is, taking into account the decisions of all parties to the conflict, which have reflexive properties and reflect the cost of resources to be protected, and the cost of the attack, is a significant feature of the proposed algorithm. As a result, the algorithm allows identifying the range of resources that are most likely to carry out cyber attacks (Fig. 9). The security assessment method is based on the assumption that the security assessment is described by Gaussian law.

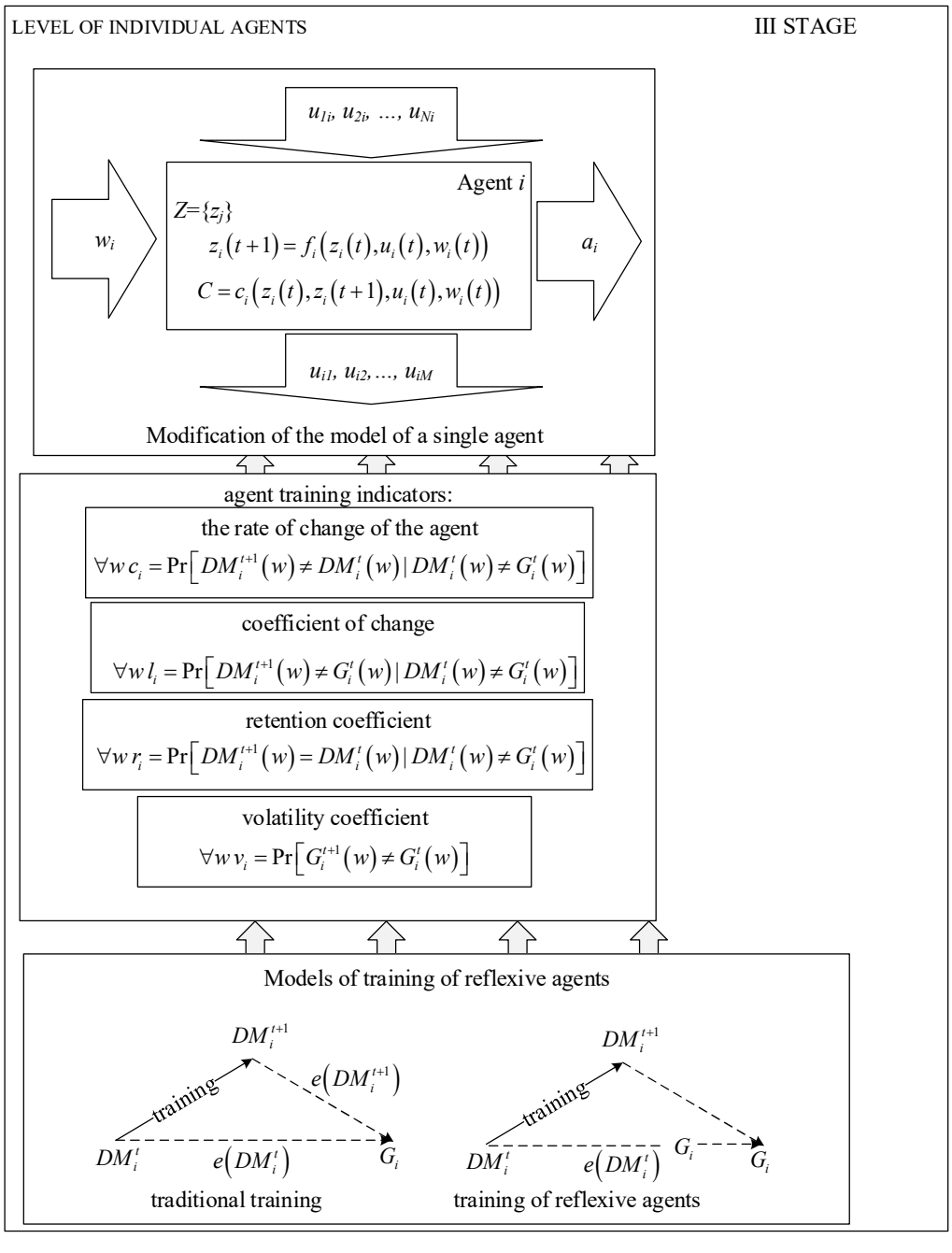

Fig. 7. Main components of the III stage of methodology construction (level of individual agents)

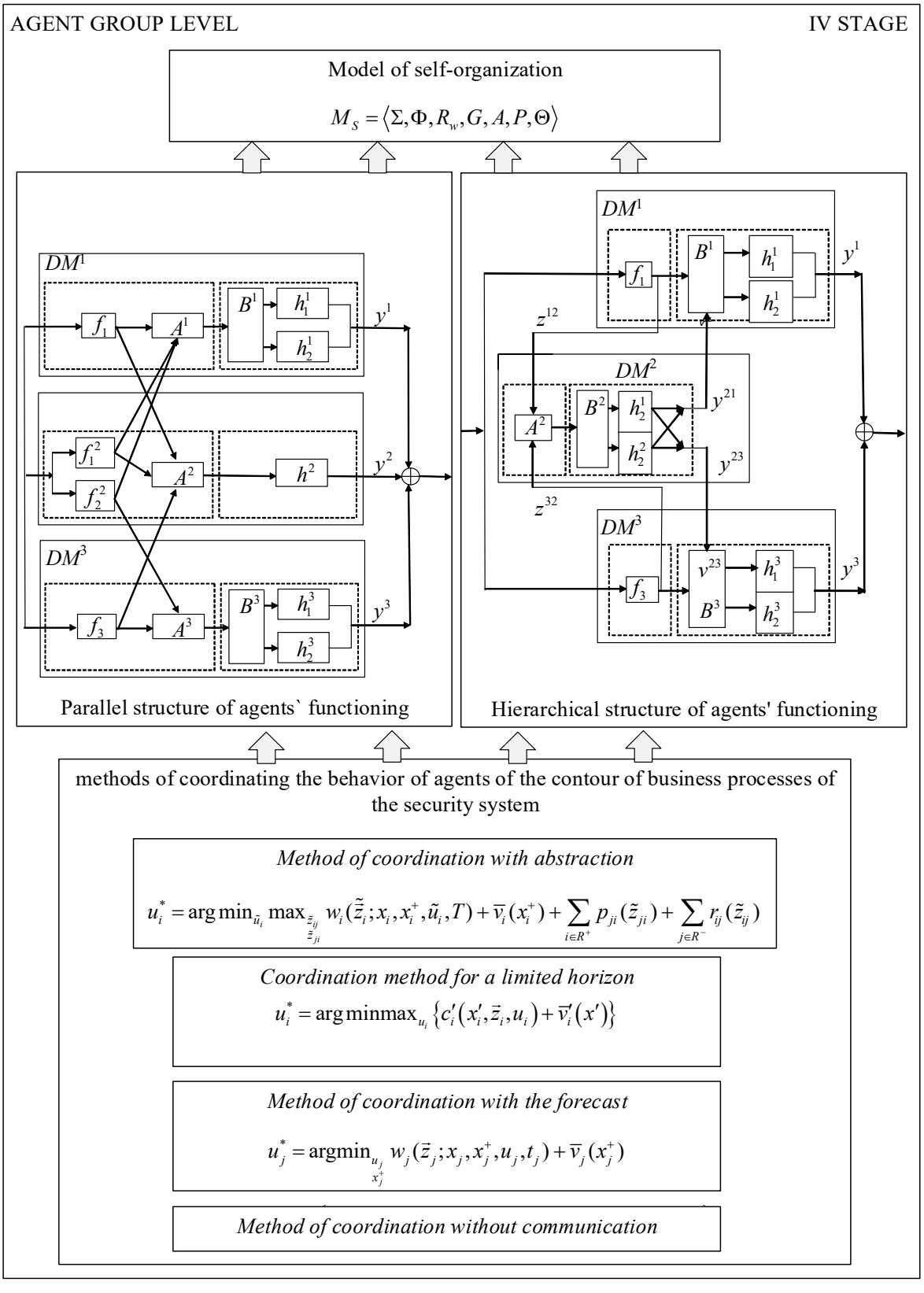

Fig. 8. Main components of the IV stage of methodology construction (level of agent group)

Notation in Fig. 8 has the following meaning: Tr_R^A – set of potential threats, the implementation of which is effective for the attacker; Tr_i – threat to the i-th information resource; P_i^A – assessment of the cost of success of the attack on the i-th resource of the business process by the attacker; C_i^A – cost of an attack on the i-th resource of the business process by the attacker; Tr_C^D – set of threats protection against is cost-effective; P_i^D – assessment of the cost of

loss of the i-th information resource for the defense party; C_i^D – cost of protection of the i-th information resource for the defense party; K_i^A – rating coefficient (importance) of implementing the threat to the i-th information resource; M – power (number of elements) of a set of selected potentially effective threats to the attacking party; K_j^D – rating coefficient (importance) of building protection of the j-th information resource.

The proposed methodology is based on the combined use of all the above set of models, methods and algorithms. It can be argued that the combined use of models, methods and algorithms leads to a synergistic effect in the modeling process. The methodology allows predicting the possible behavior of the attacker, justifying the choice of cyber threat countermeasures at the system level and calculating the required amount of investment in cybersecurity with an appropriate distribution of security components and investment time. A graphical representation of the levels of representation of models, methods and algorithms as components of the methodology for modeling agent behavior is shown in Fig. 10.

Thus, the proposed methodology for modeling the behavior of interacting agents, the basis of which is a three-level structure of modeling subjects and business processes of security systems and organizations, increases the level of security of business processes by reducing the number of hybrid threats by 1.76 times, which reduces losses by 1.65 times and increases the time to choose counteraction means by reducing the time to identify the threat online by 38 %.

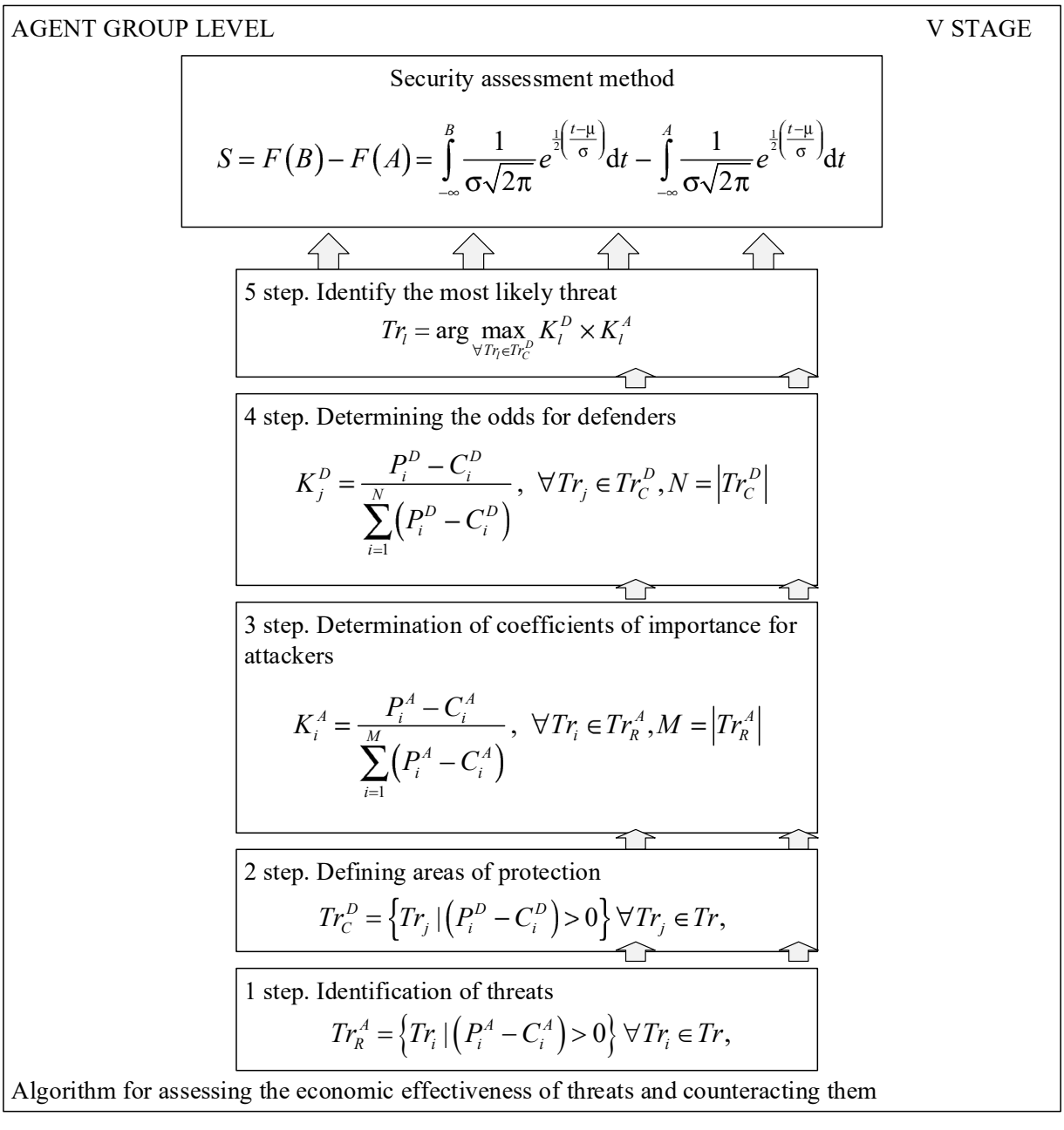

Fig. 9. Main components of the V stage of methodology construction (level of agent group)

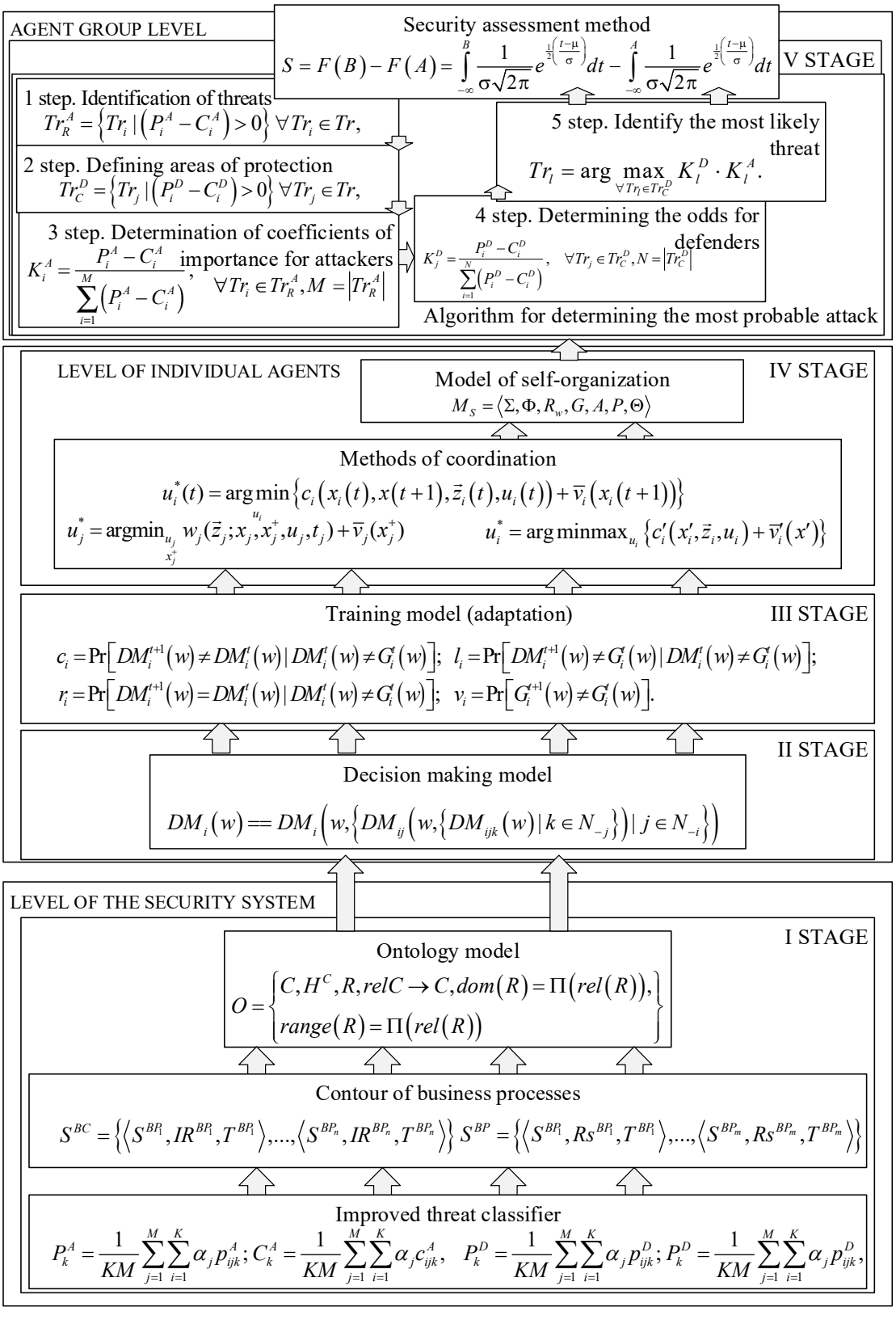

Fig. 10. Space-time structure of the methodology for modeling the behavior of interacting agents

7. Verification of the proposed methodology by simulation

To verify the behavior models developed within the proposed modeling methodology, different conditions were used to conduct and counter attacks on the business process contour. Simulation was performed for business processes of banking, as one of the systems that, on the one hand, is the most attractive for attacks, and on the other hand, has detailed business processes for the main functions of the system.

The conditions that determine the so-called basic run were considered as the basis for simulation. These conditions imply, first of all, equal capabilities of attackers and defenders and a certain basic value of the time to switch to another attack vector. The conditions for each scenario were formed on the basis of the basic run, information asymmetry of the defender/attacker's capabilities and the values of the security vector. These three conditions were chosen for the following reasons.

First, the baseline scenario shows the behavior of the system when the capabilities of the parties and the values of the attack vectors are equal. This allows for the implementation of "weakest link" (WL), as well as "wait and see" (WAS) strategies in both conditions of certainty and uncertainty in decision-making.

Second, the capabilities of defenders and attackers determine how likely attackers are to use attack vectors as part of the WL strategy, and how likely defenders are to respond to violations based on the WAS strategy. If the attacker has higher resources than the defender, he will be able to implement attacks using different vectors. On the other hand, higher capabilities of defenders mean that defenders will be able to block all incoming attacks. This means no response to violations (since they are never implemented) and, consequently, no use of the WAS strategy.

Finally, the asymmetry in the value of attack vectors makes the analysis more realistic, because in reality security vectors have different values of weights that determine the value of the resource that the attack is aimed at. Therefore, violations on a vector with a large weight can lead to greater or lesser damage to the defender's performance, depending on the value of such a vector.

The scenario space is a set of alternative conditions in relation to the conditions of the baseline run. This space includes baseline scenario conditions, asymmetric possibilities and values of the asymmetric vector relative to the baseline scenario with an uncertainty equal to zero and three levels of uncertainty classified as low, medium and high uncertainty.

The business process contours of the bank's strategic management system, the bank's business process management system, the bank's personnel management system and organizational structure, the bank's quality management system, the project management system, the risk management system and the marketing management system were considered as objects of bank system protection.

The description of the main variables used in simulation models of behavior scenarios of agents of business process contours and restrictions of the proposed models are given in [60]. A detailed description of the set of scenarios that were modeled within the proposed methodology is given in [61].

The financial costs of organizing the protection of critical infrastructure from both conventional and hybrid attacks can be significantly reduced as follows. First, in preventing errors in organizing cyber attack countermeasures, and secondly, in detecting errors when choosing the inadequate attack counteraction method and the behavior of the counteraction party in the stages preceding the implementation of the attack. The resulting goal setting should focus on finding adequate patterns of behavior of conflicting agents in the face of a possible cyber conflict, without waiting for its implementation.

Simulation of a set of scenarios of security agents' behavior was performed using the PowerSim visual system modeling environment.

The run of the baseline scenario shows that the attacks are successful, starting with vector A, as shown by the initial period (Fig. 11). However, attackers switch to the next weakest link, when the defender corrects security flaws, and the attacker receives information about the most successful attacks.

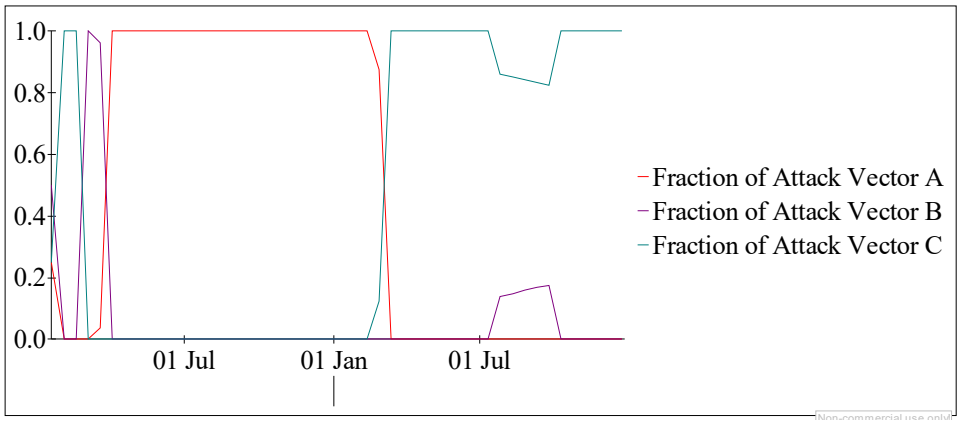

Fig. 11. Basic run. Distribution of attacks by vectors (share of total)

The purpose of the asymmetric capability scenario is to show the behavior of agents when one of the opponents has more resources than the other, and what is the impact of this behavior on successful attacks and financial results of both parties. The following assumptions are considered in the asymmetric capability scenario:

– defenders' capabilities – 1,000 units;

– attackers' capabilities – 100±20;

– values of the security vectors are the same and equal to one.

In further modeling and analysis of the behavior of interacting agents, we take into account that to successfully repel an attack requires much more capabilities than to organize and conduct it. For the parameters used in the behavior scenario modeling process, this ratio is approximately 10 to 1.

In the case of successful attacks, if the capabilities of defenders far exceed the capabilities of attackers, successful attacks do not occur. On the contrary, when the capabilities of attackers exceed a certain level corresponding to the limit level of possible reflection by defenders, attackers will constantly use all attack vectors.

Of particular interest is the behavior of interacting agents when crossing the specified ratio of attackers and defenders means.

When the ratio of attackers-defenders' capabilities is 125: 1,000, the attackers' capabilities are enough to carry out successful attacks on all vectors. At the same time, switching between attack vectors is quite intense, which does not allow the defense to react in a timely manner, identify and ensure protection of the weakest link (Fig. 12). The point of intersection of financial indicators of defenders and attackers can be interpreted as

the critical point of the breakdown of the security system. It corresponds to a state of counteraction, when the financial performance of defenders begins to decline sharply at a time when the profit of the attacking party, although slowly, increases. In other words, the capabilities of defenders are not enough to protect any resource of the business process contour.

With increased defense capabilities, it becomes possible to protect more and more resources. Fig. 13 demonstrates the emergence of a critical point of recovery of the protection system, when the financial performance of the security system begins to exceed the performance of the attacker and show a steady upward trend.

Fig. 14–16 clearly demonstrate the dynamics of the ratio of financial indicators of counteraction parties. As the defense's capabilities increase, the period of time when successful attacks are carried out becomes smaller. And at a certain ratio there comes a turning point, when defenders are able to repel more and more attacks, and this moment comes earlier (Fig. 14–16).

The obtained ratios allow estimating the required level of investment in cyber defense to partially or completely block attacks on the system. It can be assumed that the obtained ratios (when adjusting the model to the specific conditions of cyber attacks) can be used to assess the capabilities of the attacker, based on the available means of protection and the dynamics of repelling attacks.

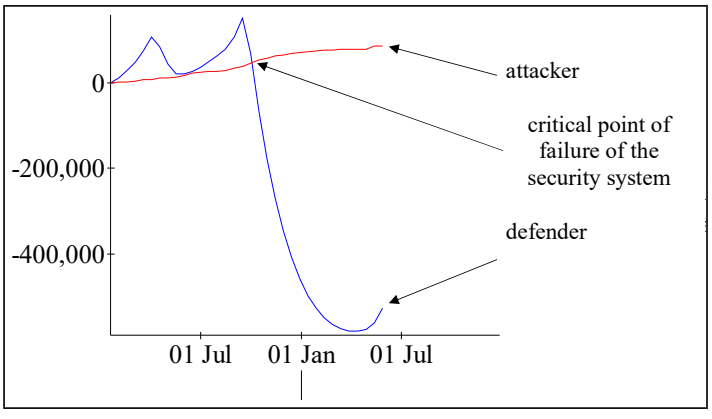

Fig. 12. Emergence of a critical point of failure of the security system with insufficient resources

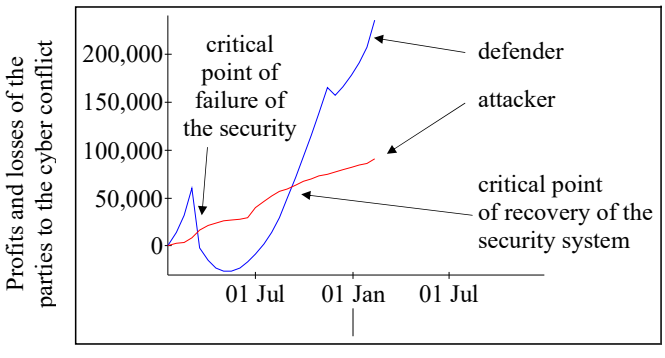

Fig. 13. Emergence of a critical point of recovery of the security system with sufficient resources

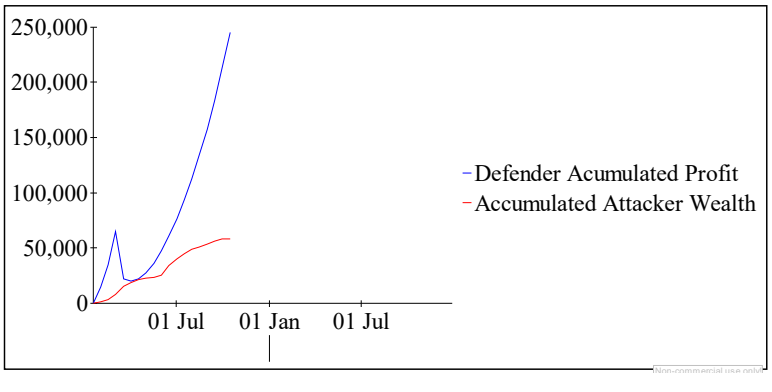

Fig. 14. Dynamics of financial indicators of counteraction parties (USD), capability ratio 92: 1,000

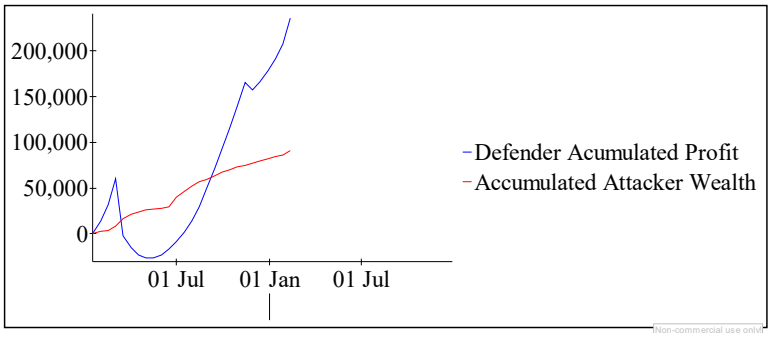

Fig. 15. Dynamics of financial indicators of counteraction parties (USD), capability ratio 93: 1,000

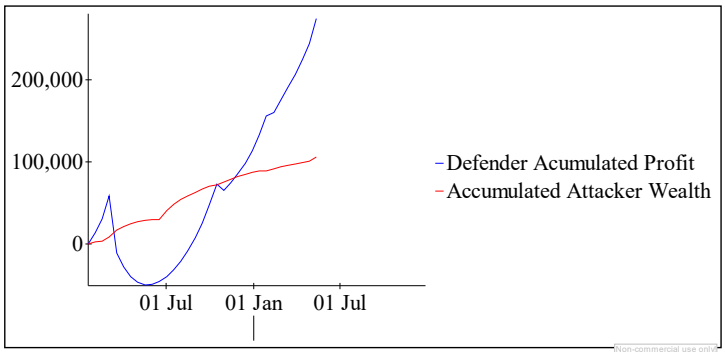

Fig. 16. Dynamics of financial indicators of counteraction parties (USD), capability ratio 94: 1,000

8. Discussion of the results of the methodology study using the proposed models, methods and algorithms

The proposed methodology with the given space-time structure allows increasing the level of security of the business process contour by reducing the number of hybrid threats. Defenders make investment decisions based on evidence of successful attacks. This means that attacks must be stopped after a while, either because they have been repelled, or attempts are being made to find another vulnerability in the security system (Fig. 17).

The main purpose of the scenario of increasing the time of switching between attacks is to increase the time of switching to another attack vector. Therefore, the defender "stores" reports of successful attacks for a longer time to extract more information from them and, as a result, reduce the uncertainty associated with future attacks (Fig. 18).

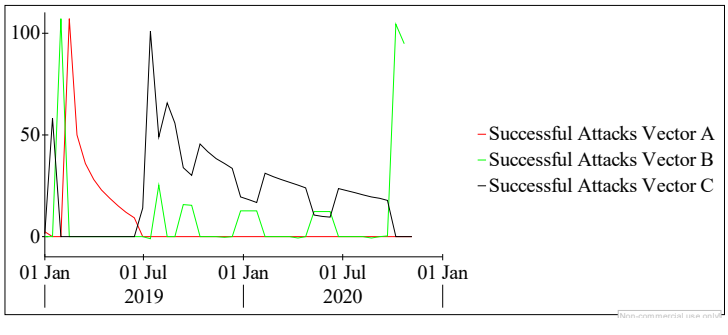

Fig. 17. Reactive response to cyber threats

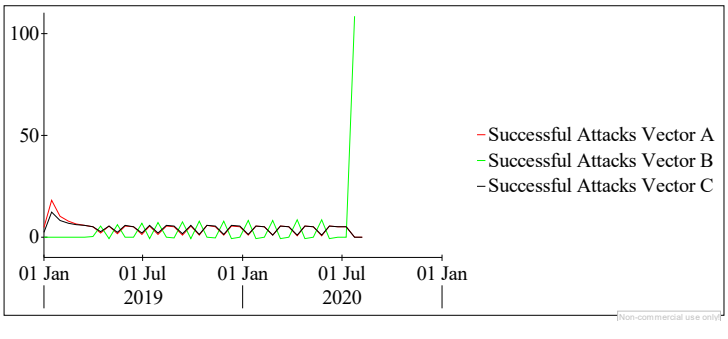

Fig. 18. Proactive response to cyber threats

Fig. 19 shows the data demonstrating that when increasing the interval for switching from one threat vector to another by 2 times, the number of successful attacks decreases by 1.76 times. A further increase in switching time has almost no effect on reducing the number of successful attacks.

With an increased security level of the business process contour due to additional funding, the switching time can be increased up to 3 times (Fig. 20).

The main purpose of the scenario of increasing the time of switching between attacks is to increase the time of switching to another attack vector. Therefore, the defender "stores" reports of successful attacks for a longer time to extract more information from them and, as a result, reduce the uncertainty associated with future attacks.

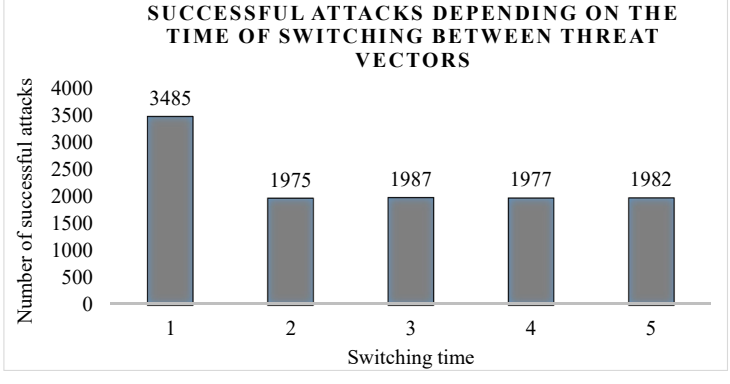

Fig. 19. Summary data on successful attacks depending on the time of switching between threat vectors

This is achieved by reducing the time to identify the threat online using a variety of models and methods of the methodology to predict the most likely threats. As a result, this reduces losses and increases the time to choose counteraction means.

The proposed methodology allows finding the minimum level of investment in protection, which provides a critical point for the recovery of the security system (Fig. 9). The implementation of scenario modeling demonstrates the relationship between the ratio of funds of counteraction sides and the dynamics of critical points of breakdown and recovery of the security system (Fig. 14–16).

The proposed model allows determining the critical point of the level of effective investment in the security system, provides effective counteraction to modern hybrid threats to the elements of the business process contour, increases the security level of the organization due to the effective level of investment in the security system. The dependence of the security level of the business process contour of the security system on the time of switching from the protection of one security vector to another was revealed. The identified dependence exists in the range of the ratio of resources of the defense and counteraction parties, in which attacks can be carried out and countermeasures can be used. This is most evident in the small range of balance between the defenders' and attackers' capabilities. Fig. 17 shows the dynamics of successful attacks in the case

of reactive response to attacks, and Fig. 18 – in proactive response, when the interval of switching from one attack vector to another increases. Fig. 19 shows the data demonstrating that when the interval for switching from one threat vector to another increases by 2 times, the number of successful attacks decreases by 1.76 times (from 3,485 to 1,975). A further increase in switching time has almost no effect on reducing the number of successful attacks.

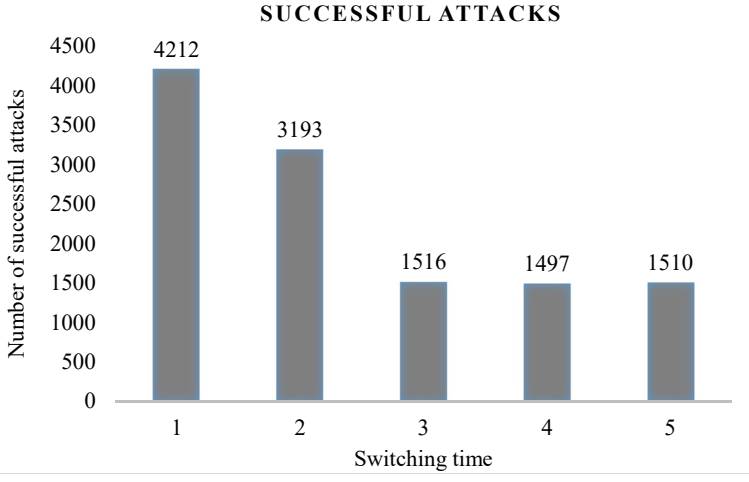

Fig. 20. Summary of successful attacks depending on the time of switching between threat vectors with increased security

Thus, the proposed methodology allows predicting the possible behavior of the attacker, justifying the choice of cyber threat countermeasures at the system level and calculating the required amount of investment in cybersecurity with an appropriate distribution of security components and investment time.

However, using it requires not only mathematical modeling, but also simulation skills. Agent behavior scenarios are built into these models, so to implement new behavior scenarios it is necessary to develop new or modify existing models, which is not always possible.

As a follow-up to this study, a situational management approach can be suggested. In contrast to the existing business process security management system, which is based on models of both business processes and models of attacks, agent behavior, etc., situational management can be considered as precedent management. The central object is the concept of the situation that combines the current state of the system, available resources and possible actions of one or another party. The situation model is the basis for building a database of situations, for which it is necessary to develop appropriate methods to supplement the description of situations, generalization and classification of situations, as well as develop a language for describing situations. The concept of scenario and its description are an integral part of precedent management. The issues of decision-making procedures, planning in the space of tasks and situations need to be implemented in security systems. It should be noted that the methods of situational management are focused on use in conditions where the construction of a mathematical model of the object or subject of management is impossible or extremely time-consuming. From the very beginning, these methods take into account the presence of a person in the control circuit and his subjectivity of perception of the processes that take place, and his characteristics in decision-making and behavior in security systems.

In the post-quantum period, with the emergence of a full-scale quantum computer, the question of what mechanisms will be able to provide preventive measures becomes acute. One of the promising areas, according to the USA NIST experts, is the use of McEliece and Niederreiter crypto-code structures. Practical algorithms for providing basic security services: confidentiality, integrity and authenticity are proposed in [57–59]. This approach, taking into account their commercial implementation, does not contain cryptocurrencies and provides not only the required level of cryptographic security, but also the reliability and efficiency of the transmitted data. Thus, the synthesis is based on the proposed methodology with promising algorithms for providing security services will significantly reduce the possibility of threats to the security of the organization's business processes.

9. Conclusions

1. Features of modeling the behavior of interacting agents of security systems in cyberconflict, which allowed determining the minimum required set of models, methods and algorithms that provide effective modeling to assess the necessary means of ensuring the appropriate level of security of business processes are revealed. Sets of models, methods and algorithms allow predicting the possible behavior of the attacker and the required amount of investment to justify the choice of countermeasures for modern threats.

2. The concept of modeling the behavior of interacting agents is developed, the basis of which is a three-level structure of modeling the subjects and business processes of the contours of the organization and security system, based on modeling the behavior of antagonistic agents. The concept can be used to predict the possible behavior of the attacker, justify the choice of cyber threat countermeasures at the system level and calculate the required amount of investment in cybersecurity with an appropriate distribution of areas and time of investment.

3. A methodology for modeling the behavior of antagonistic agents of security systems is developed, which allows predicting the possible behavior of the attacker, justifying the choice of cyber threat countermeasures at the system level and calculating the required amount of investment in cybersecurity. The space-time structure of the methodology for modeling the behavior of antagonistic agents of the security system determines the appropriate models, methods and algorithms.

4. The proposed methodology is verified on the basis of simulation modeling of three scenarios of security agents behavior: the baseline scenario, the scenario of asymmetric capabilities and the scenario of changing the time of switching from one threat vector to another. The verification demonstrated the practical possibility of applying the developed methodology to ensure the required level of protection of the business process contour with limited funds for the investment in security.

References

1. Riley, M., Elgin, B., Lawrence, D., Matlack, C. (2014). Missed alarms and 40 million stolen credit card numbers: How target blew it. Bloomberg. Available at: http://www.bloomberg.com/news/articles/2014-03-13/target-missed-warnings-in-epic-hack-of-credit-card-data
2. M-trends 2016. Mandaint: A FireEye Company. Available at: https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-mtrends-2016.pdf
3. Jajodia, S., Noel, S. (2010). Advanced cyber attack modeling analysis and visualization. Final Technical Report. Available at: https://apps.dtic.mil/dtic/tr/fulltext/u2/a516716.pdf
4. Qin, X., Lee, W. (2004). Attack Plan Recognition and Prediction Using Causal Networks. 20th Annual Computer Security Applications Conference. doi: https://doi.org/10.1109/csac.2004.7
5. Xie, P., Li, J. H., Ou, X., Liu, P., Levy, R. (2010). Using Bayesian networks for cyber security analysis. 2010 IEEE/IFIP International Conference on Dependable Systems & Networks (DSN). doi: https://doi.org/10.1109/dsn.2010.5544924
6. Fava, D. S., Byers, S. R., Yang, S. J. (2008). Projecting Cyberattacks Through Variable-Length Markov Models. IEEE Transactions on Information Forensics and Security, 3 (3), 359–369. doi: https://doi.org/10.1109/tifs.2008.924605
7. Stotz, A., Sudit, M. (2007). Information fusion engine for real-time decision-making (INFERD): A perceptual system for cyber attack tracking. 2007 10th International Conference on Information Fusion. doi: https://doi.org/10.1109/icif.2007.4408113
8. Wang, B., Cai, J., Zhang, S., Li, J. (2010). A network security assessment model based on attack-defense game theory. 2010 International Conference on Computer Application and System Modeling (ICCASM 2010). doi: https://doi.org/10.1109/iccasm.2010.5620536
9. Grunewald, D., Lutzenberger, M., Chinnow, J., Bye, R., Bsufka, K., Albayrak, S. (2011). Agent-based network security simulation. In Proceedings of The 10th International Conference on Autonomous Agents and Multiagent Systems, 3, 1325–1326. Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.387.1315&rep=rep1&type=pdf
10. Moskal, S., Wheeler, B., Kreider, D., Kuhl, M. E., Yang, S. J. (2014). Context Model Fusion for Multistage Network Attack Simulation. 2014 IEEE Military Communications Conference. doi: https://doi.org/10.1109/milcom.2014.32
11. Moskal, S., Kreider, D., Hays, L., Wheeler, B., Yang, S. J., Kuhl, M. (2013). Simulating attack behaviors in enterprise networks. 2013 IEEE Conference on Communications and Network Security (CNS). doi: https://doi.org/10.1109/cns.2013.6682726
12. Sheyner, O., Haines, J., Jha, S., Lippmann, R., Wing, J. M. (2002). Automated generation and analysis of attack graphs. Proceedings 2002 IEEE Symposium on Security and Privacy. doi: https://doi.org/10.1109/secpri.2002.1004377
13. Jha, S., Sheyner, O., Wing, J. (2002). Two formal analyses of attack graphs. Proceedings 15th IEEE Computer Security Foundations Workshop. CSFW-15. doi: https://doi.org/10.1109/csfw.2002.1021806
14. Moskal, S. F. (2016). Knowledge-based Decision Making for Simulating Cyber Attack Behaviors. Rochester Institute of Technology.
15. Kotenko, I., Man'kov, E. (2003). Experiments with Simulation of Attacks against Computer Networks. Computer Network Security, 183–194. doi: https://doi.org/10.1007/978-3-540-45215-7_15
16. Kotenko, I. (2005). Agent-based modeling and simulation of cyber-warfare between malefactors and security agents in internet. Proceedings 19th European Conference on Modelling and Simulation.
17. Kotenko, I. (2010). Agent-Based Modeling and Simulation of Network Infrastructure Cyber-Attacks and Cooperative Defense Mechanisms. Discrete Event Simulations. doi: https://doi.org/10.5772/46961
18. Kotenko, I., Doynikova, E. (2014). Security Assessment of Computer Networks Based on Attack Graphs and Security Events. Lecture Notes in Computer Science, 462–471. doi: https://doi.org/10.1007/978-3-642-55032-4_47
19. Kotenko, I., Doynikova, E. (2015). The CAPEC based generator of attack scenarios for network security evaluation. 2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS). doi: https://doi.org/10.1109/idaacs.2015.7340774
20. Milov, O., Kostyak, M., Milevsky, S., Pogasiy, S. (2019). Methods for modeling agent behavior in information and communication systems. Control, Navigation and Communication Systems. Academic Journal, 6 (58), 63–70. doi: https://doi.org/10.26906/sunz.2019.6.063
21. Yevseiev, S., Milov, O., Milevskyi, S., Voitko, O., Kasianenko, M., Melenti, Y. et. al. (2020). Development and analysis of game-theoretical models of security systems agents interaction. Eastern-European Journal of Enterprise Technologies, 2 (4 (104)), 15–29. doi: https://doi.org/10.15587/1729-4061.2020.201418
22. Yevseiev, S., Karpinski, M., Shmatko, O., Romashchenko, N., Gancarczyk, T., Falat, P. (2019). Methodology of the cyber security threats risk assessment based on the fuzzy-multiple approach. 19th International Multidisciplinary Scientific GeoConference SGEM2019, Informatics, Geoinformatics and Remote Sensing. doi: https://doi.org/10.5593/sgem2019/2.1/s07.057
23. Yevseiev, S., Aleksiyev, V., Balakireva, S., Peleshok, Y., Milov, O., Petrov, O. et. al. (2019). Development of a methodology for building an information security system in the corporate research and education system in the context of university autonomy. Eastern-European Journal of Enterprise Technologies, 3 (9 (99)), 49–63. doi: https://doi.org/10.15587/1729-4061.2019.169527
24. Yevseiev, S., Ponomarenko, V., Ponomarenko, V., Rayevnyeva, O., Rayevnyeva, O. (2017). Assessment of functional efficiency of a corporate scientific-educational network based on the comprehensive indicators of quality of service. Eastern-European Journal of Enterprise Technologies, 6 (2 (90)), 4–15. doi: https://doi.org/10.15587/1729-4061.2017.118329

25. Sun, R. (2007). The importance of cognitive architectures: an analysis based on CLARION. Journal of Experimental & Theoretical Artificial Intelligence, 19 (2), 159–193. doi: https://doi.org/10.1080/09528130701191560
26. Gilbert, N. (2004). Agent-based social simulation: dealing with complexity. Available at: http://wiki.commres.org/pds/AgentBasedModeling/AbssDealingWithComplexity.pdf
27. Carley, K. M., Prietula, M. J., Lin, Z. (1998). Design versus cognition: The interaction of agent cognition and organizational design on organizational performance. Journal of Artificial Societies and Social Simulation, 1 (3). Available at: http://jasss.soc.surrey.ac.uk/1/3/4.html
28. Helbing, D., Balietti, S. (2011). How to do agent-based simulations in the future: From modeling social mechanisms to emergent phenomena and interactive systems design. Santa Fe Institute. Available at: https://sfi-edu.s3.amazonaws.com/sfi-edu/production/uploads/sfi-com/dev/uploads/filer/bf/ee/bfee7621-d34e-438c-ae9a-cbe9346b7d85/11-06-024.pdf
29. Axelrod, R., Tesfatsion, L. (2006). Appendix A A Guide for Newcomers to Agent-Based Modeling in the Social Sciences. Handbook of Computational Economics, 1647–1659. doi: https://doi.org/10.1016/s1574-0021(05)02044-7
30. Nilsson, N. J. (1977). A production system for automatic deduction. Technical Note 148. Available at: http://www.sri.com/sites/default/files/uploads/publications/pdf/743.pdf
31. Chao, Y. R. (1968). Language and Symbolic Systems. Journal of the American Oriental Society, 88 (2), 386. doi: https://doi.org/10.2307/597363
32. Ishida, T. (1994). Parallel, Distributed and Multiagent Production Systems. Lecture Notes in Computer Science. doi: https://doi.org/10.1007/3-540-58698-9
33. Georgeff, M., Pell, B., Pollack, M., Tambe, M., Wooldridge, M. (1999). The Belief-Desire-Intention Model of Agency. Lecture Notes in Computer Science, 1–10. doi: https://doi.org/10.1007/3-540-49057-4_1
34. Bordini, R. H., Hbner, J. F., Wooldridge, M. (2007). Programming Multi-Agent Systems in AgentSpeak usingJason. Wiley Series in Agent Technology. doi: https://doi.org/10.1002/9780470061848
35. Dignum, F., Kinny, D., Sonenberg, L. (2002). From desires, obligations and norms to goals. Cognitive Science Quarterly, 2 (3–4), 407–430. Available at: https://dspace.library.uu.nl/bitstream/handle/1874/19827/dignum_02_from.pdf?sequence=1
36. Cohen, P. R., Levesque, H. J. (1990). Intention is choice with commitment. Artificial Intelligence, 42 (2–3), 213–261. doi: https://doi.org/10.1016/0004-3702(90)90055-5
37. Adam, C., Gaudou, B. (2016). BDI agents in social simulations: a survey. The Knowledge Engineering Review, 31 (3), 207–238. doi: https://doi.org/10.1017/s0269888916000096
38. Pereira, D., Oliveira, E., Moreira, N., Sarmento, L. (2005). Towards an Architecture for Emotional BDI Agents. 2005 Purtuguese Conference on Artificial Intelligence. doi: https://doi.org/10.1109/epia.2005.341262
39. Jiang, H., Vidal, J. M. (2006). From rational to emotional agents. In: Proceedings of the AAAI Workshop on Cognitive Modeling and Agent-based Social Simulation. Available at: http://jmvidal.cse.sc.edu/papers/jiang06b.pdf
40. Kennedy, W. G. (2011). Modelling Human Behaviour in Agent-Based Models. Agent-Based Models of Geographical Systems, 167–179. doi: https://doi.org/10.1007/978-90-481-8927-4_9
41. Kollingbaum, M. J. (2005). Norm-Governed Practical Reasoning Agents. University of Aberdeen. Available at: https://d1wqtxts1xzle7.cloudfront.net/4122560/10.1.1.140.9830.pdf?response-content-disposition=inline%3B+filename%3DNorm_governed_practical_reasoning_agents.pdf&Expires=1607609016&Signature=P7DWElEw3dWe3euGRJ8xm-3qVPj2zdQlNaUGqdC5RtoBYy~8r4ZTUf9iS-TyX7bnpLguKyGqdiuR964YWWpct8VTqzbUcbtfgjEJUy7LQqO4LnE7o3Gi9Jk48GGZZJJ1WTls4rdcJxbEIuV36edq~LW9NiKb1tVynLylL7EaJHuE3HixkysL26g37vixaHuysBefxcgtXmmLNB3JDs0GR-7lqn0c70LRzedugOdTGAAfbpcWIrsMEhG8jp39S4XUxjTgdU4czRuQOaBOcsRsoR8MPAL27CTg~2tvp9rBSXOu1SWurL4AgRxohSleQI0i9bt5~VZtwDtvm3u0gwTwwg__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA
42. Dignum, F. (1999). Autonomous agents with norms. Artificial Intelligence and Law, 7, 69–79. doi: http://doi.org/10.1023/A:1008315530323
43. Castelfranchi, C., Dignum, F., Jonker, C. M., Treur, J. (2000). Deliberative Normative Agents: Principles and Architecture. Lecture Notes in Computer Science, 364–378. doi: https://doi.org/10.1007/10719619_27
44. Conte, R., Castelfranchi, C. (1995). Cognitive and Social Action. Taylor & Francis, 224. doi: https://doi.org/10.4324/9780203783221
45. Sun, R. (2009). Cognitive Architectures and Multi-agent Social Simulation. Lecture Notes in Computer Science, 7–21. doi: https://doi.org/10.1007/978-3-642-03339-1_2
46. Card, S. K. (Ed.) (1983). The Psychology of Human-Computer Interaction. CRC Press, 488. doi: https://doi.org/10.1201/9780203736166
47. Byrne, M. (2007). Cognitive Architecture. Human Factors and Ergonomics, 93–113. doi: https://doi.org/10.1201/9781410615862.ch5
48. Sun, R., Peterson, T., Sessions, C. (2002). Beyond Simple Rule Extraction: Acquiring Planning Knowledge from Neural Networks. Neural Nets WIRN Vietri-01, 288–300. doi: https://doi.org/10.1007/978-1-4471-0219-9_32
49. Laird, J. E., Newell, A., Rosenbloom, P. S. (1987). SOAR: An architecture for general intelligence. Artificial Intelligence, 33 (1), 1–64. doi: https://doi.org/10.1016/0004-3702(87)90050-6
50. Laird, J. E. (2012). The SOAR Cognitive Architecture. MIT Press. doi: https://doi.org/10.7551/mitpress/7688.001.0001
51. Laird, J. E. (2012). The SOAR cognitive architecture. AISB Quarterly, 134, 1–4. Available at: https://pdfs.semanticscholar.org/a065/0855634a156db81a01dcdceff931e9f1ac04.pdf

52. Wooldridge, M., Jennings, N. R. (1995). Agent theories, architectures, and languages: A survey. Intelligent Agents, 1–39. doi: https://doi.org/10.1007/3-540-58855-8_1
53. Dolan, P., Hallsworth, M., Halpern, D., King, D., Metcalfe, R., Vlaev, I. (2012). Influencing behaviour: The mindspace way. Journal of Economic Psychology, 33 (1), 264–277. doi: https://doi.org/10.1016/j.joep.2011.10.009
54. Adam, C. (2007). Emotions: from psychological theories to logical formalization and implementation in a BDI agent. Institut de Recherche en Informatique de Toulouse. Available at: https://oatao.univ-toulouse.fr/7612/1/adam.pdf
55. Steunebrink, B. R., Dastani, M., Meyer, J.-J. C. (2010). Emotions to control agent deliberation. AAMAS '10: Proceedings of the 9th International Conference on Autonomous Agents and Multiagent Systems, 1 (1), 973–980. Available at: http://dl.acm.org/citation.cfm?id=1838206.1838337
56. Shmatko, O., Balakireva, S., Vlasov, A., Zagorodna, N., Korol, O., Milov, O. et. al. (2020). Development of methodological foundations for designing a classifier of threats to cyberphysical systems. Eastern-European Journal of Enterprise Technologies, 3 (9 (105)), 6–19. doi: https://doi.org/10.15587/1729-4061.2020.205702
57. Milov, O., Yevseiev, S., Aleksiyev, V., Berdnik, P., Voitko, O., Dyptan, V. et. al. (2019). Development of the interacting agents behavior scenario in the cyber security system. Eastern-European Journal of Enterprise Technologies, 5 (9 (101)), 46–57. doi: https://doi.org/10.15587/1729-4061.2019.181047
58. Milov, O., Yevseiev, S., Ivanchenko, Y., Milevskyi, S., Nesterov, O., Puchkov, O. et. al. (2019). Development of the model of the antagonistic agents behavior under a cyber conflict. Eastern-European Journal of Enterprise Technologies, 4 (9 (100)), 6–19. doi: https://doi.org/10.15587/1729-4061.2019.175978
59. Yevseiev, S., Korol, O., Kots, H. (2017). Construction of hybrid security systems based on the crypto-code structures and flawed codes. Eastern-European Journal of Enterprise Technologies, 4 (9 (88)), 4–21. doi: https://doi.org/10.15587/1729-4061.2017.108461
60. Yevseiev, S., Hryhorii, K., Liekariev, Y. (2016). Developing of multi-factor authentication method based on niederreiter-mceliece modified crypto-code system. Eastern-European Journal of Enterprise Technologies, 6 (4 (84)), 11–23. doi: https://doi.org/10.15587/1729-4061.2016.86175
61. Yevseiev, S., Tsyhanenko, O., Ivanchenko, S., Aleksiyev, V., Verheles, D., Volkov, S. et. al. (2018). Practical implementation of the Niederreiter modified crypto¬code system on truncated elliptic codes. Eastern-European Journal of Enterprise Technologies, 6 (4 (96)), 24–31. doi: https://doi.org/10.15587/1729-4061.2018.150903