***Представлено теоретико-ігровий підхід, який претендує на універсальний метод вирішення більшості задач в області кібербезпеки. В якості аргументів на підтвердження переваги теорії ігор виділені такі як математична обґрунтованість і доказова оптимальність прийнятих рішень, на відміну від широко використовуваних евристик, можливість розробки надійного захисту, грунтуючись на аналітичних результатах, забезпечення своєчасної реакції на кібератаки в умовах обмежених ресурсів, а також розподілений характер прийняття рішень.***

***Введено дефініції основних понять, що використовуються в задачах забезпечення безпеки на основі теоретико-ігрових моделей.***

***Перераховано особливості застосування методів теорії ігор в області кібербезпеки і сформульовані обмеження досліджень в цій області, а саме: обмеження на ігрові стратегії, одночасність ходів гравців в моделях поведінки агентів системи безпеки, невизначеність у часі здійснення ходів гравцями, невизначеність в кінцевій цілі противника, непрогнозованість подальших ходів гравців, відсутність у гравців оцінки ресурсів противника, а також його кінцевих цілей, неможливість своєчасної оцінки поточного стану гри.***

***Перерахованим проблемам безпеки поставлені у відповідність теоретико-ігрові моделі, а також визначені основні рішення, отримані в результаті застосування відповідних моделей.***

***Сформовано множину методів теорії ігор, для кожного з яких визначено відношення між моделлю гри, областю її застосування, результатом моделювання та послугами безпеки, які підтримує даний метод.***

***Визначено обмеження класичного уявлення моделей теорії ігор, необхідність подолання яких випливає з вимог забезпечення основних послуг безпеки. До таких обмежень віднесені: здатність захисника виявляти атаки, визначеність ймовірностей зміни станів до початку гри, сінхронність дії гравців, неможливість масштабованості моделі через розмір та складність системи.***

***Розроблено моделі основних задач взаємодії антагоністичних агентів систем безпеки. Моделі дозволили отримати рішення двох найбільш поширених задач в області кібербезпеки, а саме, взаємодії системного адміністратора і зловмисника при організації захисту інформаційних ресурсів. Задачі вирішені для двох різних умов – матриця гри містить вартісні оцінки ресурсів і матриця відображає ймовірності реалізації загрози. Визначено чисті і змішані стратегії для різних початкових умов, що дозволяє виключити з розгляду стратегії, що не входять в рішення.***

***Сформовано синергетичний підхід використання теоретико-ігрового моделювання з урахуванням особливостей поведінки агентів систем безпеки, заснований на аналізі різноманітності і особливостей теоретико-ігрових моделей, властивих їм обмежень і області застосувань***

***Ключові слова: теорія ігор, кібербезпека, ігри Стакельберга, ігри Неша, рівновага гри, стратегія***

UDC 004.056+519.832
DOI: 10.15587/1729-4061.2020.201418

# DEVELOPMENT AND ANALYSIS OF GAME-THEORETICAL MODELS OF SECURITY SYSTEMS AGENTS INTERACTION

**S. Yevseiev**
Doctor of Technical Sciences, Professor*
**O. Milov**
PhD, Professor*
E-mail: Oleksandr.Milov@hneu.net
**S. Milevskyi**
PhD, Associate Professor*
**O. Voitko**
PhD, Deputy Head of Department
Department of Information Technology and Information Security Employment
Institute of the Troops (Forces) Support and Information Technologies**
**M. Kasianenko**
PhD
Department of Radio Technical and Special Troops**
**Y. Melenti**
PhD
Special Department No. 2 «Tactical-Special Training, Marksmanship Training and Special Physical Training»
Juridical Personnel Training Institute for the Security Service of Ukraine Yaroslav Mudryi National Law University
Myronosytska str., 71, Kharkiv, Ukraine, 61002
**S. Pohasii**
PhD*
**H. Stepanov**
PhD, Associate Professor, Professor
Department of Air Force**
**O. Turinskyi**
PhD, Head of University
Ivan Kozhedub Kharkiv National Air Force University
Sumska str., 77/79, Kharkiv, Ukraine, 61023
**S. Faraon**
Adjunct
Department of Communications and Automated Control Systems**
*Department of Cyber Security and Information Technology
Simon Kuznets Kharkiv National University of Economics
Nauky ave., 9-A, Kharkiv, Ukraine, 61166
**National Defence University of Ukraine named after Ivan Cherniakhovskyi
Povitroflotskiy ave., 28, Kyiv, Ukraine, 03049

*Received date 21.02.2020*
*Accepted date 20.04.2020*
*Published date 30.04.2020*



## 1. Introduction

Networks have become a traditional tool in people's lives, users are very dependent on networks to provide comfortable communication and convenient access to information. Modern information and communication technologies are developing rapidly, not only in terms of complexity, but also in terms of their diversity. The growing complexity, ubiquity

and connectivity of modern information systems pose new challenges in the field of security, and cyberspace has become a platform for people with different levels of skills and all kinds of intentions (both positive and negative). Thanks to round-the-clock communication, which has become an integral part of people's daily lives, the protection of information, personal data and assets has become even more important than ever. Traditional security has come a long way towards protecting clearly defined goals, such as confidentiality, integrity, accessibility and authenticity (CIA+).

Along with the expansion of the scope of services provided by network services, the problems associated with the safe use of network services are growing. Network security is becoming a complex topic, as many new network attacks, which are becoming hybrid, are becoming more sophisticated and lead to huge losses of network resources. A crime area such as cybercrime has formed, which requires the closest attention due to the prevalence of the computer as a tool in various areas of human activity. Like other forms of crime, the causes of cybercrime are difficult to determine, however, as a rule, this is due to some factors, which include high financial gain, personal emotions and even revenge, as well as ethical, ideological, moral and environmental problems.

Most cybersecurity studies focus on either presenting a specific vulnerability or proposing a specific defense algorithm against a well-defined attack pattern. Although such cybersecurity research is important, attention should be paid to the dynamic interaction between attackers and defenders, where both sides are intelligent and can dynamically change their attack or defense strategies to defeat their opponents. This phenomenon of «cyber warfare» exists in most cases of cybersecurity in the real world [1].

It is necessary to emphasize the following. On the one hand, the weakness of traditional solutions for network security lies in their lack of a system of quantitative solutions [2].

On the other hand, security assessment [3] is an important aspect of network security; this is an assessment of confidentiality, integrity, availability, vulnerability and security risks. Network Security Measurement is a large category that includes the measurement of every aspect of network security. Risk assessment [4] is one such measure. Network security measurements include interactions between attackers and defenders, and their interactions can influence the measurement result. One of the metrics in assessing the risk for a network system is the probability of its attack. It is necessary to predict the actions of both defenders and attackers.

To solve the problems of network security, solutions based on game theory are quite often proposed, since the interaction process between attackers and defenders is considered as a game. In this case, game theory can be used in every possible scenario to predict the actions of attackers, and then to determine the decisions of defenders.

Game theory-based approaches outperform traditional cybersecurity and network privacy solutions in many ways, including the following:

1) mathematical validity and provability. Most of the traditional security solutions that are implemented either in prevention devices (for example, firewalls) or in the means of rapid response to threats (for example, antivirus programs) rely only on heuristics. Nevertheless, game theory can investigate security solutions with mathematically grounded methods, the correctness and effectiveness of which can be justified mathematically;

2) reliable protection. Based on the analytical results of applying game theory methods, reliable mechanisms can be developed to protect cyber systems from selfish behavior (insider or external attacks) by malicious users/nodes;

3) timely response. Although the adoption of a traditional security decision is rather slow due to the lack of incentives for participants, game-theoretic approaches defend the interests of defenders using basic incentive mechanisms in the context of allocating limited resources to balance perceived risks;

4) distributed solutions. Most traditional defense mechanisms make decisions centrally, rather than individually (or distributed). In network security games, a centralized approach is almost impossible because of the lack of a coordinator in an autonomous system. Using appropriate game theory models, security solutions will be implemented in a distributed manner.

These reasons favor the use of the game theory paradigm for modeling and analyzing the behavior of security systems antagonistic agents.

## 2. Literature review and problem statement

Game-theoretic analysis focuses on identifying the likely behavior of players with respect to the choice of strategy, thus determining the intended outcome of the game. It was noted in [5] that models based on game theory demonstrate advantages in productivity and cost compared to other risk management models associated with cybercrime. However, this does not take into account that in game theory, players are rarely completely rational and do not have complete information about each other's wins and strategies.The reason for this is either the fundamental impossibility of obtaining complete information, or the significant cost of obtaining it. In addition, limited rationality is an inherent characteristic of an agent (in contrast to the ideal player in theory). And besides, game theory has always imposed restrictions, which are the only way to correctly formulate the problem, and it is based on the assumption that the parties are rational, there are few of them and each player knows the goals of his opponent [6, 7].

One way to overcome the discrepancy in the rationality of the abstract player and the real agent of cyber conflict is defense games. Defense games study the interaction between attackers and defenders, which serve as the basis for making formal decisions and developing algorithms, as well as for predicting the behavior of attackers. The applicability of game theory in this case is due to the fact that it is a mathematical toolbox independent of the field of application, which can be used in any situation of interactive decision-making [8], for example, in computer and communication networks for modeling various problems. This approach includes work on modeling service disciplines [9], for TCP performance [10], and for modeling power control in a wireless communication system [11]. [12] described the application of game theory to develop protection against «denial of service» (DoS) attacks. In the field of MANET [13], cooperative and non-cooperative game-theoretic constructions were used to develop based on the reputation of the collaboration architecture.

The approach to the application of game theory related to the modeling of intrusion detection processes in computer systems should be noted. The authors of [14] used a game-theoretic structure to model intrusion detection using sampling in communication networks, and also developed sampling schemes that are optimal [15].

In general, the game-theoretic approach works with at least two players. The success of a player in choosing depends on the choice of others. In game theory, players clash with each other in turn to maximize their winnings in an attempt to achieve their ultimate goal [16]. In the area of cybersecurity, game theory has been used to determine the nature of cyber conflict. The attacker's decision-making strategies are closely related to the defender's strategies and vice versa. Cybersecurity is then modeled by at least two intelligent agents interacting in an attempt to maximize their intended goals. It should be noted that this work limits the number of players to 2, suggesting the alternation of each other's moves. In real situations of cyber confrontation, this can significantly narrow the scope of game-theoretic methods.

Going beyond the limitations inherent in this work can be considered in the works [17, 18]. It was noted in the works that the various methods available in game theory can be used for tactical analysis of cyber threat options created by both one attacker and an organized group. A key concept in game theory is the ability to explore the vast number of possible threat scenarios in a cyber system. Game theory can also provide methods for proposing several possible actions along with a predicted outcome for controlling future threats. Computers can analyze all combinations and permutations to find exceptions in general rules, unlike people who tend to overlook some possibilities. This approach allows to identify what-if scenarios that the human analyst may have overlooked.

In [19, 20], the interaction between the attacker and the network administrator is presented as a game, the modeling of which allows one to determine many strategies that lead to Nash equilibrium.

In [19], a methodology was presented for modeling the interaction between an attacking DDoS and a network administrator. This approach has shown that the ability to model and identify the intentions, objectives, and strategies of an attacker (AIOS) is important because it can lead to effective risk assessment and prediction of harm. In this paper, a stimulus-based game model for outputting AIOS was discussed. Several bandwidth parameters were used as a metric to measure the effects of attack and countermeasures, which, in turn, measures the attacker's and defender's stimulus. It was also noted in the work that the best game model to be selected depends on the degree of accuracy of the intrusion detection systems (IDS) used and the degree of correlation between the stages of the attack. The topology considered in the simulation experiment consists of 64 source hosts connected to one victim machine through 4 levels of routers. Each router is able to use a reflection mechanism as part of a security strategy.

In the model presented in [20], an attacker and a network administrator participate in a two-person stochastic zero-sum game. In this work, it was assumed that the network consists of a set of interdependent nodes whose security assets and vulnerabilities are interrelated. The concept of linear influence networks was used in the work and the interdependence between nodes was modeled using two weighted oriented graphs, one of which denoted the relationship of security assets, and the other denoted a correlation of vulnerability between nodes. The numerical example presented in the paper describes a small network of three nodes and explains the method of calculating the optimal strategies of players. However, there are no mechanisms for implementing the strategies found.

In [21], an extension of traditional approaches to the use of game theory is proposed. It addresses the issue of network security as a sequence of non-zero sum games played by an attacker and defender. This game model, called «fictitious game (FG)», assumes that players cannot accurately observe each other's previous actions. In this paper, we studied the influence of error probabilities associated with a sensory system on Nash equilibrium strategies for players, taking into account two scenarios:

a) each player knows about these error probabilities;

b) none of the players know these error probabilities.

Both classic and stochastic FP games are investigated using simulation.

A promising approach related to the introduction of dynamics and taking into account the time characteristics of the game is presented in [22]. The paper presents a game-theoretic model of developing a response to an attack on an Internet worm. The basic idea is that defenders can choose how to organize resistance and minimize the speed of the worm. An attacker can choose the optimal distribution of the scan group to maximize the speed of infection. Thus, the game will be played between the attacker and the defender. The attacker must choose the maximum speed of the worm, while the defender wants to minimize it. If we formulate the problem in this way, then it will be a game with a zero sum and a minimax problem. The optimal solution to this problem is when the defender must deploy the application evenly across the entire IP address space or in every corporate network, so the best strategy that the attacker uses is equivalent to the random scanning strategy. This work demonstrates the application of game theory for designing the locations of vulnerable and valuable hosts on the network, which should be considered a promising area of research.

In [15], a game-theoretic approach to the detection of intrusions into mobile special networks was proposed. The authors viewed intrusion detection as a game between the attacker site and the IDS hosted on the target site. The task of the attacker is to send a malicious message with the intent to attack the target node. A simulated game is a basic game that belongs to the field of multi-stage dynamic non-cooperative game. The share of publications on the dynamic theory of games in the total volume of publications is extremely insignificant, however, this direction should be recognized as promising, as evidenced by emerging scientific papers [23].

Another example of the application of game theory, which takes into account the dynamic characteristics of the game, is [24]. It presents a model for assessing the likelihood of successful attacks on a network of interdependent files and services. This paper presents a logical model that takes into account the time required to attack, crash, or repair network systems. To demonstrate the use of the game theory model, the paper gives time and topology constraints to determine if an attack or defense will succeed. The presented example describes the configuration of a high-performance web server with interdependent elements and considers the strategic actions of both the attacker and the defender.

The economic aspects of game theory in relation to security are well presented in scientific publications, given the fact that game theory was initially oriented toward economics. In [25], the problem of information security in a mobile electronic commerce network is analyzed. It is argued that the application of game theory in the field of information security is based on the hypothesis of perfect player rationality, while in reality the bulk of information security is determined by limited rationality, which is an assumption of the evolutionary game theory. The penalty parameter is introduced into the task as a parameter, which is assigned if the organization in the mobile electronic commerce network does not invest in

information security. The results of modeling the dynamics of this game made it possible to obtain the return on investment results. This can be seen as an application of evolutionary game theory to an investment strategy in network security for maximum return. It should be noted that evolutionary games are not sufficiently used in modeling cybersecurity problems.

In [26], game theory is presented in the unusual context of analyzing a proposal for an advocate organization to invest in information security. The work is focused more on information security management than on information security technologies. The paper formulates the problem of two organizations investing in security, with parameters such as investment, security and disaster risk. Based on the payout matrix, a penalty parameter has been introduced related to the refusal to invest, which ensures the rationality of investment. In conclusion, an argument is put forward in favor of encouraging organizations to invest in information security.

A taxonomy of the application of game theory in cybersecurity, consisting of four dimensions, which provide a holistic classification covering network and computer attacks, help to improve computer and network security, and language consistency with the description of the attack, was proposed in [27]. The first dimension is the attack vector, which is used to classify an attack into an attack class. The second dimension allows to classify attacks by specific targets (for example, OS: Linux: RedHat6.0). The third dimension consists of vulnerability classification and attack usage (for example, CVE/CERT). The fourth and final dimension highlight potential payloads or related effects (such as file deletion). Each dimension provides different levels of information to successfully classify and provide attack details.

A review of publications on the application of game theory in cybersecurity demonstrated the following. Almost all publications are devoted to the development of specific models for solving specific problems, emphasizing the advantages of game theory for solving problems of this class. The scope of the game theory methodology is extensive, given the fact that the classical game theory is independent of the subject area of research and applications. Not all studies analyze the applicability of the game-theoretic modeling methodology. Under these conditions, two fundamental issues are practically not addressed. The first is related to the formulation of the limitations of the game theory methodology for solving cybersecurity problems, which has its own characteristics and can set requirements for the proposed approaches and methods. The second question logically follows from the first. In the case of improper use or fundamentally impossibility to use the methodology of game theory, which methodology should be applied taking into account the features of the tasks being solved. In other words, an approach should be proposed to evaluate and select the most appropriate methodology for modeling the behavior of security systems antagonistic agents. The questions formulated determined the relevance of this study.

## 3. The aim and objectives of the study

The aim of the study is to develop and analyze the applicability of game-theoretic approaches for modeling the behavior of cybersecurity systems agents. To achieve the goal, it is necessary to solve the following tasks:

– to identify the main areas of game-theoretic approaches application for modeling the cybersecurity systems agents behavior;

– to give a formalized representation of game-theoretic models in security systems;

– to develop models of the main tasks of the interaction of security systems antagonistic agents.

## 4. Main directions of the game-theoretic approaches application for modeling the behavior of security system agents

We introduce the basic definitions of the basic concepts used in security tasks based on game theory (Table 1).

Based on the introduced definitions, we consider the mathematical foundations of conflict modeling and cooperation based on game theory. Suppose that the players are rational in their behavior, which implies their motivation in order to optimize the receipt of benefits based on the utility function.

The game follows certain rules according to which players can choose and implement a strategy from a set of different behavioral options in order to optimize the possible outcome of the game.

Formally, the game is described with $n$ players with strategic spaces $S_i$ and their payoff functions $U_j$ respectively for each player $i$ ($1<i<n$):

$$G=\{n;S_1,S_2,...,S_n;U_1,U_2,...,U_n\}. \quad (1)$$

The main features of game-theoretic approaches to modeling the behavior of cybersecurity systems agents are [17]:

– restriction of strategies when releasing games,

– simultaneous moves of players in the behavior patterns of security agents,

– players' time uncertainty,

– the uncertainty in the final goal of the enemy,

– unpredictability of further player moves,

– lack of players' assessment of enemy resources, as well as its ultimate goals,

– impossibility of timely assessment of the current state of the game.

The game is presented in a strategic/expanded form that describes the actions of the players. The strategic form of the game is formalized as follows:

$$Game=\left(P,\left(S_j\right)_{j\in P},\left(u_j\right)_{j\in P}\right). \quad (2)$$

There are many players $P$ in the game. The player $i$ can choose the strategy from $S_j$, and $U_j$ – this is the player's $i$ gain/utility. The combination of the player's selected strategies is the strategy profile, and the mixed strategy is generated from a set of pure strategies. Win function $U_j$ represents the relationship between the input space of all possible profiles and the output space of real numbers $R$.

Game-theoretic analysis focuses on identifying the likely behavior of players with respect to the choice of strategy, thus determining the intended outcome of the game. This point of view on the methods of game theory determines the spectrum of directions for their application in the field of cybersecurity.

Various types of games are used to study the actions of the defender and the attacker and to simulate the interaction between them. Table 2 presents game-theoretic models, security/privacy issues, and key solutions derived from the respective models.

Table 1

Basic definitions of the game theory concepts

| No. | Term | Definition |
|---|---|---|
| 1 | Game | A simplified formalized model of a real conflict situation of confronting the antagonistic parties of cyber conflict (defense and attack parties) with opposing interests that each side tries to satisfy using one or another strategy of actions, and in which it is impossible to come to an agreement satisfying both parties regarding the system administrator information resource |
| 2 | Player | The main character in the game who makes choices and takes action. A player may be represented by a person, machine, or group of people in a game. In security systems, the players are the parties to the attack (attacker) and defense (system administrator) |
| 3 | Action | An action is a move in a given game |
| 4 | Payment | Positive or negative reward for the player for this action in the game. For the system administrator, this may be the cost of the purchase and installation of protective equipment and programs against each of the threats that must be minimized. For an attacker, this could be a reward for damaging the adversary |
| 5 | Strategy | The action plan (behavior scenario) in the game, which the player can implement during the game. So, for the defense side, the strategy may be «Wait and See», and for the side of the attack, «the weakest link» |
| 6 | Game with full information | A game in which each player knows the moves of all other players that are already made. A game in which the player does not know the opponent's moves is called a game with incomplete information. Cyber conflict as a game is fundamentally a game with incomplete information |
| 7 | Bayesian game | A game in which information about strategies and payouts for other players is incomplete, and the player assigns a «type» to other players at the beginning of the game. Such games are called Bayesian games because of the use of Bayesian analysis in predicting the result, which may be characteristic of modeling the reflective behavior of one side or another in cyber conflict |
| 8 | Static/Strategic Game | A one-step game in which each player chooses his own action plan and decisions of all players are made simultaneously. This means that when choosing an action plan, one side of the conflict (defense or attack side) does not obtain any information about the action plan of the opposite side |
| 9 | Dynamic game | A game with more than one stage, at each of which players can review their actions. This can be seen as a consistent structure of the decision-making problems faced by players in a static game. Game sequences can be either finite or infinite. Dynamic games are a good reflection of the behavior of players in the implementation of the attack tree |
| 10 | Stochastic game | A game that includes probabilistic transitions through several states of the system. The game starts from the initial state; players select actions and receive a reward, which depends on the current state of the game, and then the game goes into a new state with probability based on the actions of the players and the current state. It can be used in the parties' assessment of the opposition of the probabilities of a multi-step attack and methods of counteracting it |

Table 2

Set of game-theoretic approaches

| Game model | Security problems | Solution |
|---|---|---|
| Static Prisoners Dilemma Game | Selfish behavior of agents on the network [28, 29], privacy on mobile social networks [30] | Nash Equilibrium |
| Zero-sum static game | Jamming and listening [31], denial of service attacks [32], trojans [33] | Nash Equilibrium |
| Stackelberg game | Cyberphysical security [36], data integrity and availability [37] | Stackelberg equilibrium |
| Coalition game | Selfishness in packet forwarding [36], listening [37] | Coalition Formation Algorithm |
| Zero-sum stochastic game | Cyberphysical Security [38], Secure Routing [39], Steganography [40] | Equilibrium (saddle point), Nash equilibrium |
| Bayesian game | Privacy trajectory [40], denial of service attack [41], survivability [42] | Bayes Nash equilibrium |
| Dynamic game | Secure Routing [43], Cyberphysical Security [38] | Saddle point (equilibrium) |
| Recurring game | Selfishness in packet forwarding [43] | Belief Based Strategy |
| Markov game | Intrusion Detection System (IDS) configuration [44], Smart-grid infrastructure protection [45], trust issue in an online social network [39] | Markov equilibrium |
| Evolution game | Selfishness in special networks [46], trust in autonomous multi-user networks [47] | Evolutionarily Sustainable Strategy (ESS) |

In game theory, players are rarely completely rational and do not have complete information about each other's wins and strategies. Therefore, modeling the decision-making process using several equations and parameters is doubtful. There is also the difficulty of quantifying value added through cybersecurity. Lack of quantification affects the decision-making process regarding security investments. Consequently, the attitude towards security varies depending

on the economic situation. This shows that the quantitative assessment of security-related concepts, such as trust, confidentiality and risk, in game-theoretic models is not an inherent property and requires additional development. Game theory also imposes restrictions, which are the only way to correctly formulate the problem, and it is based on the assumption that the parties are rational and few in number, and that each player knows the goals of his opponent [6, 7].

The problems of game theory in terms of cybersecurity risk management are further exacerbated by the following aspects. The difficulty of defining an equilibrium strategy and the difficulty of quantifying security parameters (such as risk, confidentiality, and trust), choosing the appropriate game model for a given security problem, and reaching consensus on how to interpret a mixed strategy.

The interaction between attackers and defenders is the basis for making formal decisions and developing algorithms, as well as for predicting the behavior of attackers. The applicability of game theory in this case is due to the fact that it is a mathematical toolbox independent of the field of application, which can be used in any situation of interactive decision-making [34, 38, 45, 48–52, 54, 58].

Based on the analysis [34, 38, 45, 48–52, 54, 58], the main models of game theory are presented that provide the possibility of their application to provide basic security services.

To model the interaction in the network, several game-theoretic approaches are used, such as approaches with perfect and imperfect monitoring. In a game with imperfect monitoring, player actions may not be directly observed due to noise. On the other hand, a game is considered as a game with perfect monitoring if all players know a series of past actions and the actions of other players can be observed without interference. A static game is classified as a game with imperfect information, because each participant chooses only his own strategy.

Based on the analysis [28, 29, 30, 36, 43, 46], Table 4 shows the main factors of the game for exchanging message packets in the network.

Thus, to provide basic security services based on the analysis of Table 3, 4 in game-theoretic models of cybersecurity systems, it is necessary to remove the limitations of the classical representation of game theory models:

– defender is always able to detect attacks;

– state transition probabilities are fixed before the start of the game, and these probabilities can be calculated from domain knowledge and past statistics;

– player actions are synchronous, which is not always realistic;

– most models are not scalable due to the size and complexity of the system in question.

This approach significantly affects the use of game-theoretic models and the formation of the basic principles of modeling cybersecurity systems to obtain a synergistic effect from the defender.

Table 3

Game theory methods for providing security services

| Game model | Application area | Simulation result | Security services |
|---|---|---|---|
| Zero-sum stochastic game | Integration of a robust physical space controller and an attack-resistant cyberspace controller within a defender | The iteration algorithm of the value to obtain equilibrium (saddle point) | Integrity, Confidentiality, Availability, Security |
| Static games | Physical and cyberspace integrated using payoff function | Nash equilibrium and Stackelberg equilibrium | Integrity, Confidentiality |
| Dynamic games | Discrete time LTI jamming problem | Equilibrium (saddle point of the payment matrix) | Integrity, Confidentiality, Authenticity |
| Markov games with zero sum | Players select actions that can trigger Smart Grid system state transitions | Nash equilibrium (also a Pareto optimal solution) | Confidentiality, Integrity, Accessibility, Authenticity, Involvement |
| Markov game | Determination of the optimal response of the defender in a cyber-physical environment | The iteration algorithm of the value to obtain the equilibrium (saddle) point | Confidentiality, Integrity |

Table 4

Game theory models for message packages exchange

| Game model | Key factors | Simulation Results | Basic Services |
|---|---|---|---|
| Game «Prisoner's Dilemma» | Introducing social morality to improve user privacy. Moral state is modeled as a Markov chain | Nash equilibrium is accepted in a game with incomplete and complete information | Confidentiality, Integrity |
| Joint game | Building coalitions to improve packet forwarding | Nash Formula for Pareto Optimal Solution | Confidentiality |
| Stochastic game | Transferring a packet is a Bernoulli process. The game is a repeating asymmetric game with random states | Distributed algorithm to achieve perfect balance in the games | Confidentiality, Integrity |
| Recurring game | A system of formal beliefs based on the Bayes rule for checking information of other nodes under imperfect observation | Iterative belief update algorithm for finding consistent equilibrium | Integrity, Availability |
| Evolution game | Making decisions based on limited information from other sites. Using the game to foster collaboration | The strategy of nodes is updated by comparing their winnings with a randomly selected neighbor | Confidentiality, Integrity, Availability, Authenticity |

## 5. Formalized representation of game-theoretic models in security systems

Studies of the use of game-theoretic modeling in the tasks of ensuring cybersecurity have made it possible to identify the most common game-theoretic models used in the field of security. These include Stackelberg, Nash games and signal games. The selected game models do not exhaust the entire variety of applied game-theoretic models, but are only examples of the most common applications.

Table 5 presents the main components of these games. These components determine the structure of the taxonomy of games and their models.

Table 5

Players, types, actions and utilities for three games

| Players $P$ | Types $\Theta$ | Actions $A$ | Utility $U$ | Duration $T$ |
|---|---|---|---|---|
| Stackelberg's game between the leader $L$ and follower $F$ | Typically homogeneous | $L: a_L \in A_L$<br>$F: a_F \in A_F$ | $L: U_L(a_L, a_F)$<br>$F: U_F(a_L, a_F)$ | One Step Leader-Follower Structure |
| Nash game between symmetrical players $V$ and $W$ | Typically homogeneous | $V: a_V \in A_V$<br>$W: a_W \in A_W$ | $V: U_V(a_V, a_W)$<br>$W: U_W(a_V, a_W)$ | The structure of simultaneous moves |
| Signal game between sender $S$ and the recipient $R$ | $S$ has several types $\theta \in \Theta$ | $S: a_S \in A_S$<br>$R: a_R \in A_R$ | $S$ of each type $\theta \in \Theta: U_S^{\theta}(a_S, a_R)$<br>$R: U_R(\theta, a_S, a_R)$ | One-step sender-receiver structure |

*Stackelberg game.*

Stackelberg games represent perhaps the most fundamental game-theoretic interactions, which are characterized by the following components:

1) players: $P = \{L, F\}$, where $L$ – leader, and $F$ – follower;

2) actions: actions for the player $L$ are set $a_L \in A_L$. Fig. 1 shows a 2×2 game in which $A = \{u, d\}$ and $u$ denotes an upward movement, and $d$ indicates a downward movement. Player $F$ has actions, where $t$ denotes the top, and $b$ denotes the bottom;

3) utiliy: after both players made moves, $L$ gets utility $U_L(a_L, a_F)$, and $F$ gets utility $U_F(a_L, a_F)$.

In Stackelberg's games, the follower makes a move after observing the leader's actions. Often cybersecurity models take advocate as $L$, and the attacker – $F$, assuming that the attacker will observe and respond to defensive strategies.

Stackelberg games consist of a leader $L$and follower $F$. $L$ selects an action $a_F$, and $F$ selects the best answer $BR_F(a_L)$. $L$ takes this best answer into account when choosing $a_F$. Stackelberg's cybersecurity models often see the defender as the leader, and the attacker as the follower, on the assumption that the attacker will observe and respond to the strategies chosen by the defender.

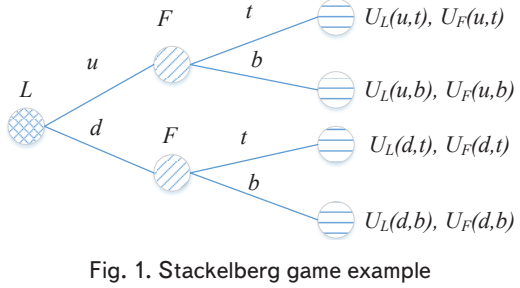



Fig. 1. Stackelberg game example

Stackelberg's games are solved backwards. Let assume that $P(S)$ denotes a set of cardinalities $S$. Then let $BR_F: A_L \to P(A_F)$ determine the best response function of the follower to the actions of the leader $BR_F(a_F)$ gives optimal $a_F$, to give the response to $a_L$. The best response function may also include a set of equally good actions. This is the reason for gaining power. The best response function is determined by:

$$BR_F(a_L) = \arg\max_{a_F \in A_F} U_F(a_L, a_F). \quad (3)$$

Based on the expectation of the best response $F$, $L$ selects the optimal action that satisfies:

$$a_L^* \in \arg\max_{a_L \in A_L} U_L(a_L, BR_F(a_L)). \quad (4)$$

Then, in balance, the actions of the players $(a_L^*, a_F^*)$, where $a_F^* \in BR_F(a_L^*)$.

*Nash game.*

While in Stackelberg games, players make moves at different times, in Nash games, players make moves at the same time. More specifically, Nash games are pre-pledged games in which each player uses his own strategy before he knows the move of the other player.

As a rule, games for two players with a preliminary commitment are displayed in matrix form.

However, Fig. 2 shows a tree diagram of a game for two players to show the difference between this game and the Stackelberg game. Players $V$ and $W$ act simultaneously or, at least, not knowing the actions of another player. The dotted line connecting two nodes for $W$ means that $W$ doesn't know which node the game has reached, because he doesn't know which move was chosen by $V$.

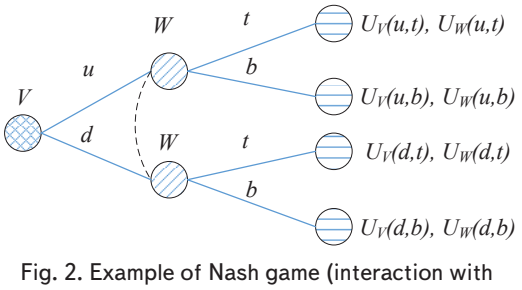



Fig. 2. Example of Nash game (interaction with a preliminary obligation)

In this case, a dashed line indicates that $W$ doesn't know which node describes the game because he doesn't know which move was chosen by $V$.

The Nash equilibrium concept requires each player to choose a strategy that is optimal, given the strategy of the other player. Let us assume that $BR_V: A_W \to P(A_V)$ is defined so that $BR_V(a_W)$ gives the set of actions for $V$, which respond optimally $W$ to the action $a_W$. Assume that $BR_W$ is defined similarly. Then a pure Nash equilibrium strategy is given by a pair $(a_V^*, a_W^*)$, such that:

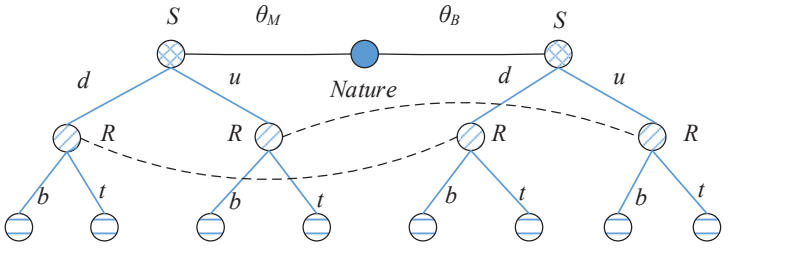
$$a_V^* \in BR_V(a_W^*), \quad (5)$$

$$a_W^* \in BR_W(a_V^*). \quad (6)$$

Nash equilibrium often requires players to choose actions according to the probability distribution. These strategies are called mixed. Mixed strategies implement the basic idea of randomizing the distribution of protection assets so as not to leave vulnerabilities open to an attacker.

*Signal games.*

Signal games, like Stackelberg games, are dynamic interactions of two players (Fig. 3). Signal games usually designate players as a sender $S$ and the recipient $R$. Sender, called type θ sender, has access to some information unknown to the recipient. The recipient learns about the type only based on the actions of the sender. For this reason, the action of the sender (in this case $a_S$) is called a message. The message does not have to match the type of sender.




$U_S^M(d,b)$ $U_S^M(d,t)$ $U_S^M(u,b)$ $U_S^M(u,t)$ $U_S^B(d,b)$ $U_S^B(d,t)$ $U_S^B(u,b)$ $U_S^B(u,t)$

$U_R(\theta_M,d,b)$ $U_R(\theta_M,d,t)$ $U_R(\theta_M,u,b)$ $U_R(\theta_M,u,t)$ $U_R(\theta_B,d,b)$ $U_R(\theta_B,d,t)$ $U_R(\theta_B,u,b)$ $U_R(\theta_B,u,t)$

Fig. 3. An example of a signal game

Signal game in which the sender $S$, having access to personal information, sends a message to the recipient $R$. The message is not subject to verification, therefore $R$ does not know the reliable information underlying. However, in the separation and partial separation of equilibria, $S$-compatible incentive transmits a message that at least partially discloses his personal information.

## 6. Development of game-theoretic models of the main tasks of the interaction of security systems antagonistic agents

Game-theoretic models of the main tasks of the interaction of security systems antagonistic agents can be implemented as a sequence of 4 stages:

1) statement of the game-theoretic problem, which consists in representing the task of organizing the protection of a computer system in terms and concepts of game theory. Players, their number and strategies, payment functions are determined. For cybersecurity systems, players are system administrators and cybercriminals. Administrator strategies involve the use of software and hardware protection tools at their disposal, and attackers' strategies are methods of attacking hardware and software resources;

2) selection and construction of a game-theoretic model of conflict (game). In other words, the question is being solved, what kind of game is it: sequential or parallel, non-coalitional or coalitional, etc.;

3) game solving (finding optimal strategies);

4) analysis of the solution and its implementation in the organization of computer system protection.

Thus, the solution to the game is the implementation of the game based on theoretical methods and software products, which makes it possible to analyze the solution of the game and use it while providing basic security services, as well as constructing a complex of information protection systems based on the interpretation of mathematical expressions of the games theory model into a security system practical mechanism.

The formulation and solution of the cybersecurity problem, in which the direct interaction of antagonistic agents takes place, seem to be a reasonable implementation of the following procedure. We consider a problem in which the cost matrix reflects the real costs or gains in value terms of the parties to the conflict. The task is to find the optimal strategy in the game between the attacker and the administrator of the computer system [56]. The optimal strategy will be in two cases when either a priori information on the frequency of occurrence of specific types of threats is available or unavailable.

Consider a zero-sum admin game with defense strategies $x_1$, $x_2$ and $x_3$ and an attacker implementing an attack vector $y_1$, $y_2$ and $y_3$. The matrix of the game is the matrix of costs that arise due to the need to purchase and install protective equipment and programs against each of the three threat vectors (Table 6). At the same time, this is the damage that an attacker causes in case of a successful attack, and, therefore, this is an attacker's gain.

The payment matrix of the game is formed on the basis of the data given in [57].

Table 6

Game matrix (thousand $)

| | $y_1$ | $y_2$ | $y_3$ |
|---|---|---|---|
| $x_1$ | 3 | 4 | 2 |
| $x_2$ | 1 | 5 | 3 |
| $x_3$ | 2 | 1 | 2 |

The expected benefit of the resource owner is made up of its capital minus the costs of the protection system and the damage from a successful attack by the attacker.

For example, if an administrator uses the $x_1$ strategy, the confrontation to the three threats $y_1$, $y_2$, $y_3$ is expressed in the cost of installing protective equipment and programs and is reduced to the fact that it is necessary to invest an amount of 9,000 $ (9,000=3,000+4,000+2,000).

Attacker using strategy $y_1$ may cause damage of $ 3,000. At the same time, the expected residual amount of funds for the owner (administrator) using the strategy $x_1$ (provided that the owner has an amount of $ 40,000) is $ 0,000–9,000–3,000= =$ 28,000. Without a protection system, the loss could have been greater since all resources would have been in the power of the attacker.

The process of searching and analyzing solutions to the formulated problem can be described as follows.

In Table 6 there are no saddle points, so the game does not have an equilibrium pair or optimal pure strategies. However, according to von Neumann's theorem, the game matrix has at least one equilibrium pair of mixed strategies.

Let the administrator use a mixed strategy $s=(p_1, p_2, p_3)$, where $p_i \geq 0$, $i=1, 2, 3$,

$$p_1+p_2+p_3=1, \quad (7)$$

and the attacker uses a mixed strategy $\sigma=(q_1, q_2, q_3)$, where $q_i \geq 0$, $i=1, 2, 3$,

$$q_1+q_2+q_3=1. \quad (8)$$

For an optimal mixed administrator strategy and for any clean attacker strategy $y_j=e_j$ payment $sAy_j^T = v\,(j=1,2,3)$, where $v$ – value of the game. Therefore,

$$\begin{aligned} &3p_1+p_2+2p_3=v,\\ &4p_1+5p_2+p_3=v, \quad (9)\\ &2p_1+3p_2+2p_3=v. \end{aligned}$$

Using (7), from here we get $p_1=2/9$, $p_2=1/9$, $p_3=2/3$ and $v=19/9$.

Similarly, for an optimal mixed attacker strategy $\sigma$ and for any pure administrator strategy $x_i=f_i$ payment $x_i^T A\sigma = v\,(i=1,2,3)$. Therefore:

$$\begin{aligned} &3q_1+4q_2+2q_3=v,\\ &q_1+5q_2+3q_3=v, \quad (10)\\ &2q_1+q_2+2q_3=v. \end{aligned}$$

They give $q_1+3q_2=0$, therefore, $q_j=0$, $j=1, 2, 3$. This contradicts (8). Consequently, one of the pure administrator strategies is missing, i. e., one of $p_i=0$, $i=1, 2, 3$.

1) $p_1=0$. The game matrix in this case has the form (Table 7):

Table 7

Game matrix (thousand $)

| | $y_1$ | $y_2$ | $y_3$ |
|---|---|---|---|
| $x_2$ | 1 | 5 | 3 |
| $x_3$ | 2 | 1 | 2 |

The first column dominates the third. Therefore, the previous matrix is reduced to a matrix (Table 8):

Table 8

Game matrix (thousand $)

| | $y_1$ | $y_2$ |
|---|---|---|
| $x_2$ | 1 | 5 |
| $x_3$ | 2 | 1 |

It is known from game theory that if $s$-mixed strategy for string (admin) and $\sigma$ – mixed strategy for the column (attacker), then there is an equilibrium pair $(s^*, \sigma^*)$ for game matrix (Table 9):

Table 9

Game matrix

| | |
|---|---|
| $A$ | $b$ |
| $C$ | $d$ |

where

$$s^*=(p, 1-p) \text{ and } \sigma^*=(q, 1-q)$$

and

$$p=(d-c)/R,\ q=(d-b)/R,\ R=a-b-c+d. \quad (11)$$

From (11) we obtain: $s=(0, 1/5, 4/5)$ and $\sigma=(4/5, 1/5, 0)$. Then we have:

$$\min\max=\min\{1/5+8/5,\ 5/5+4/5,\ 3/5+8/5\}=9/5,$$

$$\max\min=\max\{12/5+4/5,\ 4/5+5/5,\ 8/5+1/5\}=16/5.$$

As $\min\max \neq \max\min$, then there is no equilibrium point. This suggests that the assumption $p_1=0$ is not true.

2) $p_2=0$. The game matrix in this case has the form (Table 10):

Table 10

Game matrix (thousand $)

| | $y_1$ | $y_2$ | $y_3$ |
|---|---|---|---|
| $x_1$ | 3 | 4 | 2 |
| $x_3$ | 2 | 1 | 2 |

The third column dominates the first. Therefore, the previous matrix is reduced to a matrix (Table 11):

Table 11

Game matrix (thousand $)

| | $y_2$ | $y_3$ |
|---|---|---|
| $x_1$ | 4 | 2 |
| $x_3$ | 1 | 2 |

From (11) we obtain: $s=(1/3, 0, 2/3)$ and $\sigma=(0, 0, 1)$. Then we have:

$$\min\max=\min\{3/3+4/3,\ 4/3+2/3,\ 2/3+4/3\}=2,$$

$$\max\min=\max\{2, 3, 2\}=3.$$

As $\min\max \neq \max\min$, then the equilibrium point is absent and therefore, in reality $p_2=0$.

3) $p_3=0$. The game matrix in this case has the form (Table 12):

Table 12

Game matrix (thousand $)

| | $y_1$ | $y_2$ | $y_3$ |
|---|---|---|---|
| $x_1$ | 3 | 4 | 2 |
| $x_2$ | 1 | 5 | 3 |

The first column dominates the second. Therefore, the previous matrix is reduced to a matrix (Table 13):

Table 13

Game matrix

| | $y_1$ | $y_3$ |
|---|---|---|
| $x_1$ | 3 | 2 |
| $x_2$ | 1 | 3 |

According to (11) we get: $s=(2/3,1/3,0)$ and $\sigma=(1/3,0,2/3)$. Therefore:

$$\min\max=\min\{6/3+1/3,\ 8/3+5/3,\ 4/3+3/3\}=7/3,$$

$$\max\min=\max\{3/3+4/3,\ 1/3+6/3,\ 2/3+4/3\}=7/3.$$

As min max = max min, then $(s, \sigma)$ – equilibrium point.

Therefore, the optimal administrator strategy against the three attacker strategies is to use the strategy $x_1$ during 2/3 of the resource's work time and strategy $x_2$ for 1/3 of the time.

The search for a solution to the formulated problem of game theory, performed using the Gambit software package [58], fully confirmed the solution found. In addition, a solution was obtained for a mixed attacker strategy. It consists of using a strategy $y_1$ for 1/3 of the time and $y_3$ during 2/3 of the game time.

The game matrix or payment matrix implies that its elements are winnings or losses of opponents. However, a whole class of problems has formed, where the elements of the payment matrix are the probabilities of the threat or the probability of repelling the attack. Consider the statement of the problem and the analysis of the resulting solution in this case.

Assume that entries in the game matrix represent the probabilities of the administrator using the computer system of three strategies (lines $x_1$, $x_2$, $x_3$) against five threats (columns $y_A$, $y_B$, $y_C$, $y_D$, $y_E$).

We will consider as an example a game with the following payment matrix (Table 14). The initial data are the results of assessing the probability of the implementation of various threats based on weighting factors presented in the classifier [59].

Table 14

Payment matrix

| | $y_A$ | $y_B$ | $y_C$ | $y_D$ | $y_E$ |
|---|---|---|---|---|---|
| $x_1$ | 0.3 | 0.6 | 0.4 | 0.5 | 0 |
| $x_2$ | 1 | 0 | 0 | 0 | 0 |
| $x_3$ | 1 | 0.5 | 0 | 0 | 1 |

The initial data are: the absence of a priori frequency information on the types of threats and the availability of such information. We define the existence of pure strategies. The equilibrium pair (row, column) of pure strategies is the saddle point in Table 14, which is the minimum in the row and the maximum in the column. In Table 14 there is no gray point. Thus, the analysis of Table 14 showed that in this game both an equilibrium pair and a pair of optimal pure strategies are absent. However, any game has at least one equilibrium pair of mixed strategies [60].

Since each number of column $y_C$ is not more than a number in the same row of columns $y_B$ or $y_D$, then column $y_C$ dominates the columns $y_B$ and $y_D$. Therefore, both columns $y_B$ and $y_D$ can be eliminated from the game matrix without changing the equilibrium pair for the game matrix specified in Table 14. Similarly, column $y_E$ dominates the column $y_A$, and column $y_A$ can also be eliminated from the game matrix.

As a result, we have the following game matrix (Table 16):

Table 16

Game matrix

| | |
|---|---|
| 0.4 | 0 |
| 0 | 0 |
| 0 | 1 |

On the other hand, each number in row 1 in the matrix above is not less than the number in the same column of row 2, that is, row 1 dominates row 2. Therefore, row 2 can be removed from the aforementioned game matrix without changing the equilibrium pair (Table 17):

Table 17

Game matrix

| | |
|---|---|
| 0.4 | 0 |
| 0 | 1 |

The final matrix of the game is given in Table 18.

Table 18

Game matrix

| | $y_C$ | $y_E$ |
|---|---|---|
| $x_1$ | 0.4 | 0 |
| $x_3$ | 0 | 1 |

Given the ratio (11) and taking $a=0.4$, $b=c=0$ and $d=1$, we get $R=1.4$, $p=1/1.4=5/7$, $q=1/1.4=5/7$.

Thus, $s^*=\sigma^*=(5/7, 2/7)$.

Therefore, in the game from Table 14 the best strategy for defending the five threats is to use a strategy $x_1$ during 5/7 resource operating time and strategy $x_3$ for 2/7 time.

Now a priori information about the frequency of realization of threats is known. Suppose five threats appear with frequencies (0.1; 0.3; 0.3; 0.1; 0.2).

Efficiency for a clean strategy $x_1$ is equal to:

$$0.3\cdot0.1+0.6\cdot0.3+0.4\cdot0.3+0.5\cdot0.1+0\cdot0.2=0.38.$$

Similarly, efficiency for a clean strategy $x_2$ is equal to 0.1, and for a clean strategy $x_3$ – $1\cdot0.1+0.5\cdot0.3+1\cdot0.2=0.45$.

Therefore, the optimal net strategy for the administrator is the strategy $x_3$.

## 7. Discussion of the results of game-theoretic modeling of the security system agents behavior processes

The analysis of the use of game-theoretic modeling of the behavior of agents of security systems, the principles of building models and their limitations makes it possible to increase the security level of cyber systems based on the existing restrictions and analysis results (Tables 3, 4). Fig. 4 shows a synergistic approach to the use of game-theoretic modeling taking into account the particular behavior of security system agents.

Analysis of Fig. 4 defines goals, objectives, and areas of application of game-theoretic modeling of the security system agents behavior. These goals are determined by the tasks and areas of application of the considered methods (the last column of Fig. 4). The application of game theory methods allows the selection of appropriate attack and defense strategies based on typical threats of the KDD99 technique [61]. In general, the solution of these tasks provides the required level of security.

Game-theoretic models allow you to create many relevant tasks to provide basic security services: confidentiality, integrity, accessibility, authenticity. Thus, the same model can provide the solution to several security tasks, and vice versa, the same problem can be solved using different models. Because of this, in practice, it is necessary to determine the necessary subset of game models that support the solution of the entire set of security tasks, or a selected subset of them.

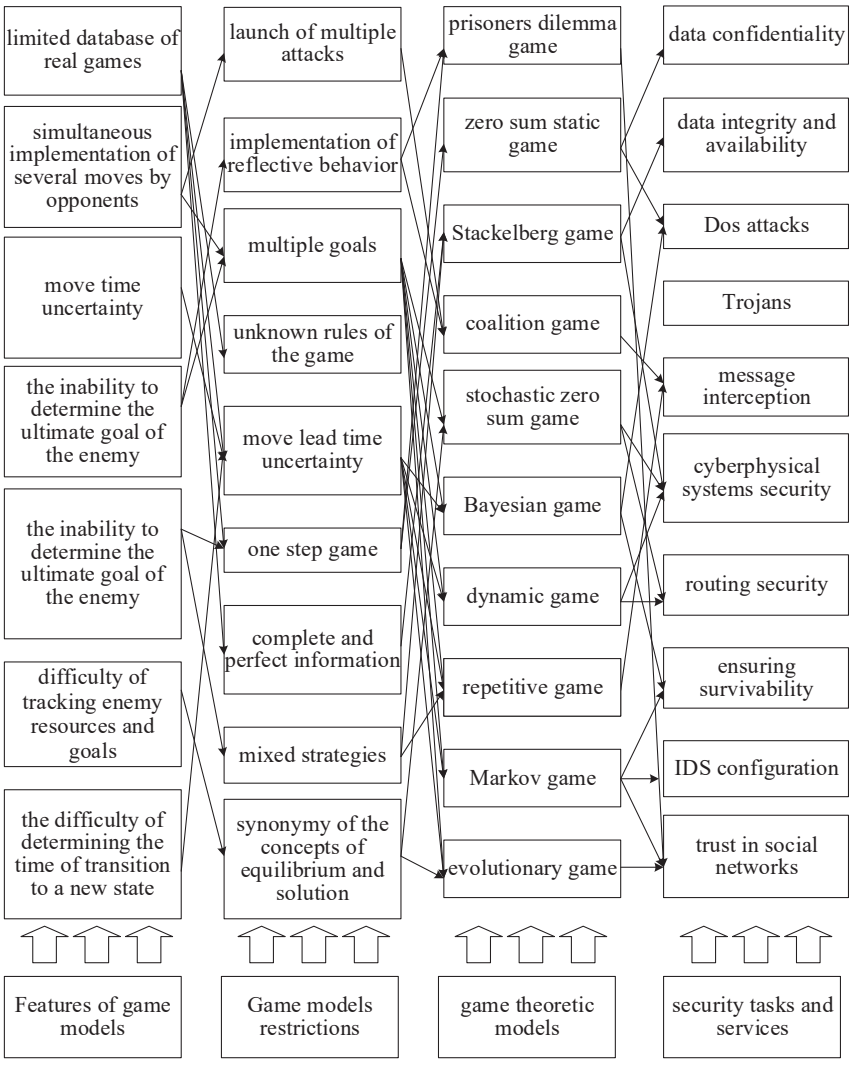



Fig. 4. Synergetic approach of game-theoretic modeling

The choice of appropriate models will be determined by the restrictions characteristic to certain game models. The main limitations of the classical models of game theory follow from basic assumptions, namely, the assumption of definiteness of the ultimate goal of the game, the synonymy of the concepts of «solving the game» and «balance», the awareness of the players about the opponent's resources, the ability of the players to construct a payment matrix, as well as the assumption of a clearly fixed sequence of players' steps that are not dependent on time. The sets of game models presented in Fig. 4 are characterized by the reflection of certain restrictions in the model, which dictates their choice for solving security problems.

These restrictions follow from the features of game models that describe the behavior of players, namely, the ability of a player to detect attacks, a predetermined sequence of moves for each of the players, the probability of behavior change for games with mixed strategies, the lack of scalability of the model in size and the complexity of the task for certain game-theoretic models.

This approach significantly affects the use of game-theoretic models and the formation of the basic principles of modeling cybersecurity systems to obtain a synergistic effect from the defender.

Analysis of Fig. 4 allows to conclude that the advantages of using game theory in the field of cybersecurity can not always be realized due to differences between the real field of cybersecurity and traditional game domains [55]. A significant obstacle to the use of game-theoretic modeling of the processes of behavior of antagonistic agents of security systems is the set of limitations organically inherent in game theory.

Thus, in real conditions, there are many characteristics that contradict the simple implementation of standard search methods.

Game theory allows to determine the optimal strategy, but does not give any recommendations regarding the implementation of this strategy. The list of standard terms used in game theory does not include the term «behavior». In other words, game theory works more at the strategic level, not dropping to the operational level. Due to this, it does not take into account the peculiarities of behavior and the real characteristics of the players. Therefore, to model the behavior, reflect the reflective characteristics of the players and deviate from the principle of rationality in making decisions, different approaches from game theory should be used. Game theory models can be used to solve particular problems of behavior modeling without claiming the status of the main modeling methods. This situation confirms the thesis that the breadth of the problem is achieved, most likely, by increasing the level of abstraction and moving away from taking into account the characteristics of real players, their behavior, goals and methods of achieving them.

The revealed limitations inherent in the game-theoretic methodology for modeling the behavior of agents of security systems emphasize the fact that this methodology is not universal, although it has a wide scope. The consequence of this is the need to compare the specified methodology with other methodologies used for the indicated purposes.

The choice of a particular methodology should be based on a comparison of the most common modeling methodologies.

Thus, it is proposed to conduct a comparison according to the following criteria:

1) the time and effort required to apply the methodology of modeling and designing the current model with the participation of future users;

2) user requirements. The amount of technical knowledge and the level of training necessary for the user to understand and use the model;

3) studying time. Time and effort for a typical user to study the designed model and the rules for its use;

4) model flexibility. The simplicity with which a developer can change the model to include a new variable or change the variables used;

5) number of existing analog models with functions that can be adapted to be used as part of the behavior model of security agents;

6) transparency. The simplicity with which the user can discover in the model everything that can affect the simulation results.

The results of the comparison of various methodologies are presented in Table 19. It should be noted that the first three criteria should be low, and the last three criteria should be high.

Table 19

Compliance of modeling methodologies with comparison criteria

| | Time to create a model | User requirements | Study time | Flexibility | Availability of model library | Transparency |
|---|---|---|---|---|---|---|
| Game theory | L | L–H | L–H | M | H | L–H |
| Agent Modeling | M–H | L–M | L–M | M–H | L–M | M–H |
| Dynamic systems | M | H | H | M | M | M |
| System dynamics | L | L | L | H | L | H |
| Data Driven Models | M | M | L | M | M | H |

*Note: L – low, M – medium, H – high.*

Based on a set of comparison criteria for agent behavior modeling methodologies, system dynamics may turn out to be an alternative to game-theoretic modeling of agent behavior. The advantages of system-dynamic modeling also speak in favor of this choice. The methodology of system-dynamic modeling allows [62–65]:

– to detect the emergent properties of the investigated system behavior. System-dynamic models provide a way to study the formed behavior of agents based on the relatively simple rules of behavior of an individual agent. This approach allows to obtain and further study the synergistic properties of antagonistic agents in the process of cyber conflict;

– to determine the most important parameters in the system dynamics: it is necessary to determine the set of input data in order to understand their influence on the output data. The system-dynamic model allows you to evaluate the impact of each input parameter on the result of the system's functioning and rank them depending on the degree of influence, and subsequent analysis of the model's sensitivity will support the decision to include one or another factor in the model;

– to prepare quantitative assessments of qualitative ideas: systemic dynamic models allow the user to convert a qualitative understanding of agent interactions into quantitative assessments of the effectiveness of the implementation of a particular scenario of behavior in the process of cyber conflict;

– to predict the long-term consequences of decisions for a certain circuit of business processes;

– to support the use of the model and provide system administrators with a set of tools for organizing training for personnel in decision-making in difficult conditions of cyber conflict. In particular, system dynamics is a method for improving learning in complex security systems, especially large infrastructure projects. The study of complex dynamic systems requires not only technical means to create mathematical models, since these tools are applied both to human behavior and to physical and technical systems.

The results obtained from the analysis of the comparison table are explained primarily by the selection of appropriate comparison criteria. These criteria reflect the basic requirements on the part of developers of security agent behavior models. It should be borne in mind that for other subject areas and other tasks, the set of comparison criteria can be changed, which will lead to different selection results.

The second factor influencing the results of the comparison is the subjective nature of the assessments of the conformity of a particular methodology to the established criteria. In addition, these estimates are purely qualitative in nature, and the boundaries between the low, medium, and high values of compliance with the criterion are not fixed.

The subjective choice of criteria and their values determine not only the features of the proposed approach, but also its limitations. As ways to address these shortcomings of the approach to justifying and choosing a modeling methodology, the following can be proposed.

First of all, the use of expert assessment methods that provides quantitative assessments of the rationale for the choice, namely, the determination of the required number of experts and the degree of consistency of their assessments, which allows to talk about the stability of the group assessment of the chosen methodology. As the second way, allowing passing to a quantitative assessment of the justification of a choice, one can use the theory of fuzzy sets that transform the qualitative values of the criteria into quantitative estimates for their subsequent processing. It should be noted that the use of fuzzy sets in the field of cybersecurity is mainly associated with the assessment of risks of threats.

## 8. Conclusions

1. The features of the application of game theory methods in the field of cybersecurity are determined. These include, first of all, the limitation or complete lack of a database of the results of the application of game-theoretic approaches in the field of cybersecurity, the simultaneous functioning of players in the process of ensuring security. In addition, the absence of restrictions on the time taken to complete moves; lack of information about the ultimate goal of the enemy; the overall dynamism of the game, expressed in the change of actions of each of the players; the impossibility of tracking changes in enemy resources, etc. These features determine the main areas of application of game-theoretic modeling in security systems. The main directions of the application of methods and models of game theory, the security of cyber-physical systems, the security of communications, the modeling of the security system agents behavior are highlighted.

2. Some of the most common game-theoretic models used to ensure cybersecurity and confidentiality of information are presented, namely Stackelberg games, Nash games and signal games. The selected game models do not exhaust the entire variety of applied game-theoretic models, but are only examples of the most common applications. For each of the games, its formal expression is given, containing the actions of the players, the utility function, the time characteristics

of the game. Each of the mentioned games is presented in a detailed graphic form in the form of a game tree, which allows to clearly present the main idea of the game and its dynamics.

3. Models of the main tasks of the interaction of antagonistic agents of security systems have been developed. The developed models are used to solve two characteristic security tasks. The first task is to find the optimal strategy in the game between the attacker and the administrator of the computer system. The cost matrix of the players was formed taking into account real costs or gains in value terms of the parties to the conflict. For the generated cost matrix, the absence of an equilibrium pair or optimal pure strategies is determined. In accordance with von Neumann's theorem, an equilibrium pair of mixed strategies was found, consisting of the following. The optimal administrator strategy against the three strategies of the attacker is to use one of the strategies used by him for 2/3 of the resource's time and the other strategy for 1/3 of the time. The third strategy of the system administrator was not optimal for any actions of the attacker. The mixed strategy for the attacker turned out to be similar, demonstrating that he had one suboptimal strategy. The search for a solution to the formulated problem, performed using the Gambit software package, fully confirmed the solution found analytically.

The second task suggested that the elements of the payment matrix are the probabilities of a threat or reflection of an attack. The search for the optimal strategy was carried out in the conditions of accessibility or inaccessibility of a priori information about the frequency of occurrence of specific types of threats. In the first case, the optimal pair of mixed strategies was determined, while in the second case, the pure strategy turned out to be optimal.

References


1. Attiah, A., Chatterjee, M., Zou, C. C. (2018). A Game Theoretic Approach to Model Cyber Attack and Defense Strategies. 2018 IEEE International Conference on Communications (ICC). doi: https://doi.org/10.1109/icc.2018.8422719
2. Alpcan, T., Baser, T. An intrusion detection game with limited observations. Available at: https://www.tansu.alpcan.org/oldhomepage/papers/isdg06.pdf
3. Security measurement. White Paper. Available at: http://www.psmsc.com/Downloads/TechnologyPapers/SecurityWhitePaper_v3.0.pdf
4. He, W., Xia, C., Wang, H., Zhang, C., Ji, Y. (2008). A Game Theoretical Attack-Defense Model Oriented to Network Security Risk Assessment. 2008 International Conference on Computer Science and Software Engineering. doi: https://doi.org/10.1109/csse.2008.1651
5. Yazar, Z. (2002). A Qualitative Risk Analysis and Management Tool - CRAMM. SANS.
6. Aigbokhaevbolo, O. (2011). Application of Game Theory to Business Strategy in Undeveloped Countries: A Case for Nigeria. Journal of Social Sciences, 27 (1), 1–5. doi: https://doi.org/10.1080/09718923.2011.11892900
7. Manshaei, M. H., Zhu, Q., Alpcan, T., Bacşar, T., Hubaux, J.-P. (2013). Game theory meets network security and privacy. ACM Computing Surveys, 45 (3), 1–39. doi: https://doi.org/10.1145/2480741.2480742
8. Akinwumi, D. A., Iwasokun, G. B., Alese, B. K., Oluwadare, S. A. (2018). A review of game theory approach to cyber security risk management. Nigerian Journal of Technology, 36 (4), 1271. doi: https://doi.org/10.4314/njt.v36i4.38
9. Kesselman, A., Leonardi, S. (2012). Game-theoretic analysis of Internet switching with selfish users. Theoretical Computer Science, 452, 107–116. doi: https://doi.org/10.1016/j.tcs.2012.05.029
10. Akella, A., Seshan, S., Karp, R., Shenker, S., Papadimitriou, C. (2002). Selfish behavior and stability of the internet: a game-theoretic analysis of TCP. Proceedings of the 2002 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications – SIGCOMM '02. doi: https://doi.org/10.1145/633025.633037
11. Alpcan, T., Basar, T., Dey, S. (2004). A power control game based on outage probabilities for multicell wireless data networks. Proceedings of the 2004 American Control Conference. doi: https://doi.org/10.23919/acc.2004.1386817
12. Bencsth, B., Buttyn, L., Vajda, I. (2003). A game based analysis of the client puzzle approach to defend against dos attacks. In SoftCOM 2003 11th International conference on software, telecommunications and computer networks, 763–767.
13. Michiardi, P., Molva, R. (2002). Core: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks. IFIP Advances in Information and Communication Technology, 107–121. doi: https://doi.org/10.1007/978-0-387-35612-9_9
14. Murali Kodialam, Lakshman, T. V. (2003). Detecting network intrusions via sampling: a game theoretic approach. IEEE INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE Cat. No.03CH37428). doi: https://doi.org/10.1109/infcom.2003.1209210
15. Patcha, A., Park, J.-M. (2004). A game theoretic approach to modeling intrusion detection in mobile ad hoc networks. Proceedings from the Fifth Annual IEEE SMC Information Assurance Workshop, 2004. doi: https://doi.org/10.1109/iaw.2004.1437828
16. Alazzawe, A., Nawaz, A., Bayaraktar, M. M. (2006). Game theory and intrusion detection systems.
17. Hamilton, S. N., Miller, W. L., Ott, A., Saydjari, O. S. (2002). Challenges in applying game theory to the domain of information warfare. Proceedings of the 4th Information survivability workshop (ISW-2001/2002).
18. Hamilton, S. N., Miller, W. L., Ott, A., Saydjari, O. S. (2002). The role of game theory in information warfare. Proceedings of the 4th information survivability workshop (ISW- 2001/2002).
19. Liu, P., Zang, W., Yu, M. (2005). Incentive-based modeling and inference of attacker intent, objectives, and strategies. ACM Transactions on Information and System Security, 8 (1), 78–118. doi: https://doi.org/10.1145/1053283.1053288

20. Nguyen, K. C., Alpcan, T., Basar, T. (2009). Stochastic games for security in networks with interdependent nodes. 2009 International Conference on Game Theory for Networks. doi: https://doi.org/10.1109/gamenets.2009.5137463
21. Nguyen, K. C., Alpcan, T., Basar, T. (2009). Security Games with Incomplete Information. 2009 IEEE International Conference on Communications. doi: https://doi.org/10.1109/icc.2009.5199443
22. Chen, Z. (2007). Modeling and defending against internet worm attacks. Georgia Institute of Technology.
23. Hryshchuk, R. V. (2013). Dyferentsialno-ihrovi modeli ta metody modeliuvannia protsesiv kibernapadu. Kyiv, 411.
24. Bursztein, E., & Goubault-Larrecq, J. (2007). A Logical Framework for Evaluating Network Resilience Against Faults and Attacks. Advances in Computer Science – ASIAN 2007. Computer and Network Security, 212–227. doi: https://doi.org/10.1007/978-3-540-76929-3_20
25. Sun, W., Kong, X., He, D., You, X. (2008). Information Security Problem Research Based on Game Theory. 2008 International Symposium on Electronic Commerce and Security. doi: https://doi.org/10.1109/isecs.2008.147
26. Sun, W., Kong, X., He, D., You, X. (2008). Information Security Investment Game with Penalty Parameter. 2008 3rd International Conference on Innovative Computing Information and Control. doi: https://doi.org/10.1109/icicic.2008.319
27. Hansman, S., Hunt, R. (2005). A taxonomy of network and computer attacks. Computers & Security, 24 (1), 31–43. doi: https://doi.org/10.1016/j.cose.2004.06.011
28. Charles, A. K., Pissinou, N. (2010). Mitigating selfish misbehavior in multi-hop networks using stochastic game theory. IEEE Local Computer Network Conference. doi: https://doi.org/10.1109/lcn.2010.5735709
29. Charles, A. K., Pissinou, N., Busovaca, A., Makki, K. (2010). Belief-free equilibrium of packet forwarding game in ad hoc networks under imperfect monitoring. International Performance Computing and Communications Conference. doi: https://doi.org/10.1109/pccc.2010.5682295
30. Xiaohui Liang, Xu Li, Tom H. Luan, Rongxing Lu, Xiaodong Lin, and Xuemin Shen. 2012. Morality-driven data forwarding with privacy preservation in mobile social networks. IEEE Tran. Vehic. Technol. 61, 7 (Sep. 2012), 3209-3222.
31. Ara, M., Reboredo, H., Ghanem, S. A. M., Rodrigues, M. R. D. (2012). A zero-sum power allocation game in the parallel Gaussian wiretap channel with an unfriendly jammer. 2012 IEEE International Conference on Communication Systems (ICCS). doi: https://doi.org/10.1109/iccs.2012.6406109
32. Spyridopoulos, T., Karanikas, G., Tryfonas, T., Oikonomou, G. (2013). A game theoretic defence framework against DoS/DDoS cyber attacks. Computers & Security, 38, 39–50. doi: https://doi.org/10.1016/j.cose.2013.03.014
33. Kamhoua, C. A., Kwiat, L., Kwiat, K. A., Park, J. S., Zhao, M., Rodriguez, M. (2014). Game Theoretic Modeling of Security and Interdependency in a Public Cloud. 2014 IEEE 7th International Conference on Cloud Computing. doi: https://doi.org/10.1109/cloud.2014.75
34. Minghui Zhu, Martinez, S. (2011). Stackelberg-game analysis of correlated attacks in cyber-physical systems. Proceedings of the 2011 American Control Conference. doi: https://doi.org/10.1109/acc.2011.5991463
35. Djebaili, B., Kiennert, C., Leneutre, J., Chen, L. (2014). Data Integrity and Availability Verification Game in Untrusted Cloud Storage. Decision and Game Theory for Security, 287–306. doi: https://doi.org/10.1007/978-3-319-12601-2_16
36. Akkarajitsakul, K., Hossain, E., Niyato, D. (2013). Cooperative Packet Delivery in Hybrid Wireless Mobile Networks: A Coalitional Game Approach. IEEE Transactions on Mobile Computing, 12 (5), 840–854. doi: https://doi.org/10.1109/tmc.2012.46
37. Saad, W., Zhu Han, Basar, T., Debbah, M., Hjorungnes, A. (2009). Physical layer security: Coalitional games for distributed cooperation. 2009 7th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks. doi: https://doi.org/10.1109/wiopt.2009.5291619
38. Zhu, Q., Basar, T. (2011). Robust and resilient control design for cyber-physical systems with an application to power systems. IEEE Conference on Decision and Control and European Control Conference. doi: https://doi.org/10.1109/cdc.2011.6161031
39. Johnson, B., Schöttle, P., Böhme, R. (2012). Where to Hide the Bits? Decision and Game Theory for Security, 1–17. doi: https://doi.org/10.1007/978-3-642-34266-0_1
40. Jin, X., Pissinou, N., Pumpichet, S., Kamhoua, C. A., Kwiat, K. (2013). Modeling cooperative, selfish and malicious behaviors for Trajectory Privacy Preservation using Bayesian game theory. 38th Annual IEEE Conference on Local Computer Networks. doi: https://doi.org/10.1109/lcn.2013.6761339
41. Liu, Y., Feng, D., Lian, Y., Chen, K., Zhang, Y. (2013). Optimal Defense Strategies for DDoS Defender Using Bayesian Game Model. Lecture Notes in Computer Science, 44–59. doi: https://doi.org/10.1007/978-3-642-38033-4_4
42. Kamhoua, C. A., Kwiat, K. A., Park, J. S. (2012). Surviving in Cyberspace: A Game Theoretic Approach. Journal of Communications, 7 (6). doi: https://doi.org/10.4304/jcm.7.6.436-450
43. Ji, Z., Yu, W., Liu, K. J. R. (2010). A Belief Evaluation Framework in Autonomous MANETs under Noisy and Imperfect Observation: Vulnerability Analysis and Cooperation Enforcement. IEEE Transactions on Mobile Computing, 9 (9), 1242–1254. doi: https://doi.org/10.1109/tmc.2010.87
44. Shen, D., Chen, G., Blasch, E., Tadda, G. (2007). Adaptive Markov Game Theoretic Data Fusion Approach for Cyber Network Defense. MILCOM 2007 - IEEE Military Communications Conference. doi: https://doi.org/10.1109/milcom.2007.4454758
45. Ma, C. Y. T., Yau, D. K. Y., Rao, N. S. V. (2013). Scalable Solutions of Markov Games for Smart-Grid Infrastructure Protection. IEEE Transactions on Smart Grid, 4 (1), 47–55. doi: https://doi.org/10.1109/tsg.2012.2223243

46. Shivshankar, S., Jamalipour, A. (2015). An Evolutionary Game Theory-Based Approach to Cooperation in VANETs Under Different Network Conditions. IEEE Transactions on Vehicular Technology, 64 (5), 2015–2022. doi: https://doi.org/10.1109/tvt.2014.2334655
47. Kamhoua, C. A., Pissinou, N., Makki, K. (2011). Game Theoretic Modeling and Evolution of Trust in Autonomous Multi-Hop Networks: Application to Network Security and Privacy. 2011 IEEE International Conference on Communications (ICC). doi: https://doi.org/10.1109/icc.2011.5962511
48. He, F., Zhuang, J., Rao, N. S. V. (2012). Game-theoretic analysis of attack and defense in cyber-physical network infrastructures. Proceedings of the 2012 Industrial and Systems Engineering Research Conference.
49. He, F., Zhuang, J., Rao, N. S. V., Ma, C. Y. T., Yau, D. K. Y. (2013). Game-theoretic resilience analysis of Cyber-Physical Systems. 2013 IEEE 1st International Conference on Cyber-Physical Systems, Networks, and Applications (CPSNA). doi: https://doi.org/10.1109/cpsna.2013.6614252
50. Ma, C. Y. T., Rao, N. S. V., Yau, D. K. Y. (2011). A game theoretic study of attack and defense in cyber-physical systems. 2011 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). doi: https://doi.org/10.1109/infcomw.2011.5928904
51. Gupta, A., Langbort, C., Basar, T. (2010). Optimal control in the presence of an intelligent jammer with limited actions. 49th IEEE Conference on Decision and Control (CDC). doi: https://doi.org/10.1109/cdc.2010.5717544
52. Shoukry, Y., Araujo, J., Tabuada, P., Srivastava, M., Johansson, K. H. (2013). Minimax control for cyber-physical systems under network packet scheduling attacks. Proceedings of the 2nd ACM International Conference on High Confidence Networked Systems – HiCoNS'13. doi: https://doi.org/10.1145/2461446.2461460
53. Ma, C. Y. T., Yau, D. K. Y., Lou, X., Rao, N. S. V. (2013). Markov Game Analysis for Attack-Defense of Power Networks Under Possible Misinformation. IEEE Transactions on Power Systems, 28 (2), 1676–1686. doi: https://doi.org/10.1109/tpwrs.2012.2226480
54. Zonouz, S., Haghani, P. (2013). Cyber-physical security metric inference in smart grid critical infrastructures based on system administrators' responsive behavior. Computers & Security, 39, 190–200. doi: https://doi.org/10.1016/j.cose.2013.07.003
55. Goryashko, A. (2014). Game theory: from analysis to synthesis (survey of the markets design results). Cloud of Science, 1 (1), 112–154.
56. Shing, M.-L., Shing, C.-C., Chen, K. L., Lee, H. (2011). A Game Theory Approach in Information Security Risk Study. 2010 International Conference on E-business, Management and Economics IPEDR, 3, 201–203.
57. Petrenko, S., Simonov, S., Kislov, R. (2003). Informatsionnaya bezopasnost': ekonomicheskie aspekty. Jet Info, 10 (125).
58. McKelvey, R., McLennan, A., Turocy, T. (2002). Gambit: Software Tools for Game Theory.
59. Yevseiev, S., Rzayev, K., Mammadova, T., Samedov, F., Romashchenko, N. (2018). Classification of cyber cruise of informational resources of automated banking systems. Cybersecurity: Education, Science, Technique, 2 (2), 47–67. doi: https://doi.org/10.28925/2663-4023.2018.2.4767
60. Fon Neyman, D., Morgenshtern, O. (1970). Teoriya igr i ekonomicheskoe povedenie. Moscow: Nauka, 983.
61. Özgür, A., Erdem, H. (2016). A review of KDD99 dataset usage in intrusion detection and machine learning between 2010 and 2015. doi: https://doi.org/10.7287/peerj.preprints.1954v1
62. Milov, O., Voitko, A., Husarova, I., Domaskin, O., Ivanchenko, Y., Ivanchenko, I. et. al. (2019). Development of methodology for modeling the interaction of antagonistic agents in cybersecurity systems. Eastern-European Journal of Enterprise Technologies, 2 (9 (98)), 56–66. doi: https://doi.org/10.15587/1729-4061.2019.164730
63. 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
64. 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
65. 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