Design of security protection and management systems based on game theory

Serhii Toliupa[1,*,†], Serhii Buchyk[1,†], Volodymyr Nakonechnyi[1,†], Mykola Brailovskyi[1,†] and Serhii Shtanenko[2,†]

[1] *Taras Shevchenko National University of Kyiv, 60 Volodymyrska str., 01601 Kyiv, Ukraine*

[2] *Military Institute of Telecommunication and Information Technologies named after the Heroes of Kruty, 45/1 Knyaziv Ostrozkyh str., 01011 Kyiv, Ukraine*

Abstract

Currently, much attention is paid to the issues of information security. Telecommunication systems, which have been actively developing recently, are the arteries of modern global information systems. The information circulating in such systems is of significant value and is therefore vulnerable to various violations and abuses. The development of network technologies is accompanied by increased requirements for information security and the choice of the optimal level of protection systems. Many researchers propose to use the game theory framework as a mathematical basis for designing, building, and analyzing information security systems. Game theory is a formal approach designed to analyze the interaction between several participants in a process that have different interests and make decisions. The use of game theory in modeling decision-making processes has various approaches that are currently not systematic and sometimes contradict each other. Therefore, there is a need to develop methods of rapid (adaptive) information security management, depending on the availability of a priori information about the possibility of attacks by an attacker and the strategy implemented by him to create unauthorized access to an information resource. Game theory allows us to offer recommendations for creating a strategy for managing the operation of security and intrusion prevention systems.

Keywords

information security, game theory, optimal strategy, system security, offender system, decision-making, intrusion detection system, attack

1. Introduction

In this paper, we will consider two approaches to the application of game theory: the use of game theory methods to optimize the choice of information security and security management. In many situations, while doing the design of information security systems there can be a need for the development and implementation of decisions in conditions of uncertainty. Uncertainty may have a different nature. So, uncertain is the planned actions of the hackers which aim to decrease the efficiency of protection systems; uncertainty can refer to situations of risk in which the information network management system, which makes decisions on the implementation of the protection system, can establish not only all possible outcomes of decisions but the probability of possible conditions of their appearance. Design conditions affect the decision-making subconsciously, regardless of the actions of the subject that makes a decision. When aware of all the consequences of possible solutions, but without knowing their accuracy, it is clear that decisions are made in conditions of uncertainty. The basic perspective of the analysis theory of the decision-making processes at the design stage of information protection systems is game theory. The application of game theory in modeling the decision-making processes has different approaches, which currently are not systematic and sometimes collide between themselves. Therefore, the study of this subject is an *actual scientific issue.*

2. The main part

Despite significant advances in information security, there are still difficulties in preventing intrusions into the information system. An analysis of network attacks shows that protection actions are most often taken after the service performance has already been affected. This is due to the difficulty of assessing the future scale of the attack and applying the appropriate defense measure [1, 2].

To increase the accuracy of attack prediction and detection, an intrusion detection system must collect heterogeneous information about the protected system, as well as store and process a large amount of data. Using a

CPITS-II 2024: Workshop on Cybersecurity Providing in Information and Telecommunication Systems II, October 26, 2024, Kyiv, Ukraine

* Corresponding author.
† These authors contributed equally.
tolupa@i.ua (S. Toliupa);
buchyk@knu.ua (S. Buchyk);
nvc2006@i.ua (V. Nakonechnyi);
bk1972@ukr.net (M. Brailovskyi);
shsergei@ukr.net (S. Shtanenko)

0000-0002-1919-9174 (S. Toliupa);
0000-0003-0892-3494 (S. Buchyk);
0000-0002-0247-5400 (V. Nakonechnyi);
0000-0002-3148-1148 (M. Brailovskyi);
0000-0001-9776-4653 (S. Shtanenko)

filtering system in the absence of an attack results in a decrease in server performance and possible false filter triggering. Quite often, the creation of an effective protection system is faced with insufficient computing power. Thus, the task of optimizing the resources spent on maintaining the performance of the system of protection against network attacks at a high level arises [3, 4].

One of the solutions to this problem is to minimize the resources spent on maintaining information security at times when the activity of the attacker is insignificant. To this end, an intrusion detection system should use dynamic methods that allow for prompt detection and prevention of security breaches, i.e., the information security system should use a mathematical model that allows for the selection of the necessary set of security tools at any given time, providing reliable protection and at the same time requiring a minimum amount of resources.

In recent years, domestic and foreign works have shown a tendency to expand the existing mathematical approaches to the selection of information security system parameters. For example, various authors propose the following mathematical methods for analyzing and optimizing an information security system [5, 6]: methods of mathematical statistics; methods based on the use of Petri nets; mathematical apparatus of the theory of random processes; methods based on the theory of automata; methods based on the theory of fuzzy sets; methods based on the use of neural networks; methods of expert systems; mathematical apparatus of game theory [7, 8].

Statistical intrusion detection methods apply a well-proven mathematical statistics apparatus to the behavior of the subjects of the analyzed system. First, statistical profiles are formed for all subjects. The components of such a profile may include various parameters, such as total traffic per unit of time, the number of denials of service, the ratio of incoming traffic to outgoing traffic, the number of unique requests to the system, etc. Any deviation from the reference profile is considered a security breach. The main disadvantages of this approach are the following. First, intrusion detection systems based on statistical methods are not sensitive to the order of events in the protected system: in some situations, the same events, depending on the order of their occurrence, may be characteristic of abnormal or normal activity. Secondly, in some cases, it can be difficult to set thresholds for the monitored characteristics to identify anomalous activity. Underestimating the threshold leads to false positives, and overestimating it leads to missed intrusions. In addition, the attacker often uses individual approaches for each defense system, which makes the use of statistical methods less effective [9].

2.1. Design of security protection

Any information processing system consisting of various hardware and software tools can be viewed as a unique complex with its characteristics. The complexity of the effective dynamic formation of observation parameters lies in the fact that the size of the search area exponentially depends on the power of the initial set of observed parameters.

Various intelligent methods can be used in intrusion detection systems to generate a set of observed parameters. Many researchers propose to use the game theory framework as a mathematical basis for designing, building, and analyzing information security systems. Game theory is a formal approach designed to analyze the interaction between several participants in a process that have different interests and make decisions.

Any information security system involves two parties: the attacking party and the defending party (information security system), which have opposing interests. In [5], it is proposed to use the mathematical apparatus of game theory to solve the problem of choosing means of protection against unauthorized access to information in an automated system. The mathematical formulation of the problem in the form of a linear programming problem with Boolean variables is also performed there. In the mathematical formulation, the cost of protection means is introduced. The constraints of the task take into account the requirements of the classes of protection against unauthorized access in automated systems.

In [8], an overview of theoretical game methods used in solving information security problems is given. The paper considers an approach to designing intrusion detection systems using the mathematical apparatus of matrix games for two players. The proposed model takes into account the cost of system resources for organizing protection.

Paper [6] considers the possibilities of using multi-step games with incomplete information in building systems of protection against DoS attacks. It is proposed to present the problem in the form of a game of two parties: the defending party (A) and the attacking party (B). The task of the defending party is to minimize its losses due to the actions of the attacking party. The task of party B is to maximize profit. The paper points out that the main feature of such a game is that functions describing the behavior of the parties in the short term are used as strategies. It is proposed to select a variety of functions for each task individually, based on statistical data, external constraints, and common sense.

When analyzing the issues of protection against various security threats, it is advisable to consider the actions of two parties: the defense (information system) and the offender. The entirety of security threats can be considered as an intruder: the actions of individuals with different goals, large-scale planned attacks, and accidental impacts on the system. Such models, where there are two or more opposing parties, are typical of game theory [10]. If the options of actions (strategies) of each party are known, as well as the gain (or loss) from each of the options, it is possible to formulate a mathematical model of the situation in the form of a model of a non-coalition antagonistic game (for example, a matrix game). Based on the formulated task, it is possible to obtain optimal strategies for the attacking and defending parties that require a minimum of resources [11].

Consider the interaction between an intrusion detection system and an attacker as a non-coalition endgame. Suppose that the defense party A and the attacker B have a finite number of strategies n_B and n_A, which corresponds to reality, since the defense party always has a limitation on the number of possible response options, and the attacker has a limitation on the number of options for organizing an attack.

For example, in [6], it is proposed to use strategies for defense ("ignore suspicious activity", "increase monitoring"); and for the attacker, many strategies can be considered ("complete the attack", "continue without pause", "pause the attack"). A set of player strategies $s = (s_A, s_B)$, where $s_A \in S_A$, $s_B \in S_B$ set of situations. Functions ω_A and ω_B player winnings are defined on a variety of situations $S = S_A \times S_B$.

The solution to a non-coalition game is an equilibrium situation, but not necessarily in pure strategies. It is known that every finite antagonistic game has at least one equilibrium situation in mixed strategies. When analyzing information security systems, it makes sense to consider mixed strategies under the assumption that the system's operation lasts for a considerable time, i.e., attack and defense iterations are repeated many times [12]. In this case, the strategies are used by the parties with some non-deterministic regularity and the costs/income accumulate over time. The mixed strategy of players *A* and *B* is the full set of probabilities of using their pure strategies:

$$P_A = \{p_{A_1}, p_{A_2}, \dots, p_{A_n}\},$$
$$P_B = \{p_{B_1}, p_{B_2}, \dots, p_{B_n}\}.$$

In a non-coalition game, each player uses his or her pure strategies independently of the other, so in a mixed situation $p = (P_A, P_B\}$ probability $p(s)$ of the emergence of a situation $s = (s_A, s_B)$ is equal to the product of the probabilities of both players using their pure strategies, i.e. $p(s) = p(s_A, s_B)$.

Let's find the average win (loss) of players. In the case of the mathematical expectation of player *A* win in a mixed situation $p = (P_A, P_B\}$ is defined as follows:

$$W_A(p) = w_A(P_A, P_B) = \sum_{s \in S} w_A(s) p(s) =$$
$$= \sum_{s_1 \in S_A} \sum_{s_2 \in S_B} w_A(s_1, s_2) p_A(s_A)(p_B(s_B)),$$

where S_A and S_B are many possible situations of players *A* and *B*, respectively, w_A is the function of the information security system's gain (or, in fact, loss or cost) if the information security system has chosen a strategy s_1, and the offender—the strategy s_2.

The player's (information security system violator's) winnings are generally determined in the same way.

How can you determine the winnings of players in this case? The intrusion detection system provides a lot of parameters at any given time using sensors [13]. Each attack can be represented as a sequence of iterations. After each step, the intrusion detection system tries to "predict" the next steps of the intruder. Each step of the intruder generates a certain type of activity that can be detected by the system's sensors. If the analysis unit recognizes the activity as suspicious, the set of basic observed parameters must be expanded. Let the set of additional monitoring parameters be $M_{S_{\text{add}}} = \{x_1, x_2, \dots, x_n\}$, and the cost of additional resources spent on monitoring them over time $t - C_A(t)$. Let's assume that the cost of observation is directly proportional to the time of observation. If the monitoring of an extended set of parameters is carried out during the time t_m, then the cost of additional observation costs will be

$$C_A(t) = \sum_{i=1}^{n} c_i t_m,$$

where n is the number of additional monitoring parameters, c_i is the cost of monitoring the i^{th} parameter. When making a decision to ignore a possible attack, the information security system does not incur the cost of additional monitoring.

Let's estimate the costs of the information security system violator. If the decision is made to terminate the attack, the attacker does not incur additional costs, and if the decision is made to continue the attack, the attacker's costs depend on the number k of generated requests to the protected system $C_B = gk$, where g is the cost of generating one request.

In case of a successful attack, the information security system suffers losses c_A^*, and the offender wins c_B^*. The costs of the protection system when implementing each of the possible strategies consist of the costs of organizing protection $C_A(t) = \sum_{i=1}^{n} c_i t_m$ and losses from possible security breaches c_A^*. Similarly, the gain of the infringer consists of the gain from the breach of the information security system c_B^* and because of the cost of conducting attacks C_B.

For the analyzed intrusion detection system, it is assumed that with the increase of additional monitoring parameters, the probability of detecting an attack increases. However, determining the exact dependence of successful attack detection on the number and set of monitoring parameters, as well as on the monitoring time, requires an experimental study for each type of information security system.

As noted, every finite non-coalition game has at least one equilibrium situation in mixed strategies. The equilibrium situation can be found by standard game theory methods described in [8].

It should also be borne in mind that. The peculiarity of the information conflict of the information security operational management system and the peculiarity of the offender trying to carry out unauthorized access (UA) is that the opposing parties, who have several ways of acting, can apply them repeatedly, choosing the best way [14, 15]. Based on information about the actions of the opposing party.

At each step of conflict resolution is not a final state but some payment function. Traditional game approach to the analysis of the violator's actions fails to take into account multiple steps of conflict and does not reflect the dependence of the modes of action of the parties from the opposite direction, and the known conflict approach based on the calculation of the final probability of system stay in a state of winning to a given point in time does not reflect the multiplicity of actions of the parties and unqualified finality of the conflict at each step [16, 17].

2.2. Information security management

Therefore, there is a need to develop methods for rapid (adaptive) management of information security depending

on the availability of a priori information about the possibility of attacks from the intruder and the strategy of creating the *UA* implemented by him.

To describe the current status of the conflict let's use the indicator of the security of the system $a_{ij} = P_{sec}$ while implementing in it the i^{th}, $i \in I = \{1,2,...,n\}$, strategy (way) of protection and the application of the j^{th}, $j \in \mathcal{J} = \{1,2,..., m\}$ strategy (way) of creating a safety contour, m and n are the number of security strategies and creation of security measure implemented in the SS (security system) and the system of the intruder (SoI) accordingly.

Let's name the subsystem of operational management of the information protection as Party *A* and the system to counteract this protection as Party *B*, and the a_{ij}—the win of Party *A* (the loss of Party *B*) in a situation (*i, j*). The traditional gaming approach to the analysis of security systems assumes that the parties are aware of the matrix of the game and the finite set of strategies of the violator, but it is unknown which strategy is implemented in a particular situation. In this case, a matrix game can be formalized in the situation of a choice of protection strategies under conditions of uncertainty. However, this approach does not reflect the dynamics of conflict and the possibility of a purposeful selection of protection strategies at each step depending on information about the system action of the offender [18]. Therefore, it is proposed to describe the conflict using the model of a stepper matrix game with lag and errors in the awareness of the parties about the actions of the offender (matrix-game process). Let us note: T_{PS} (T_{SoI}) time of a single implementation of its pure strategy by the party *A*(*B*); t_{PS} (t_{SoI}) is reaction time of the party *A*(*B*), which is equal to the time interval from the start of implementation of the strategy by the party *B*(*A*) to the moment of implementation of appropriate strategy by the party *A*(*B*).

We assume that parties are aware of: the matrix game $\mathbf{A} = (a_{ij})_m^n$, the set of active strategies *I*, *J*, and the assessment of the values of T_{PS} (T_{SoI}) and t_{PS} (t_{SoI}); the matrix of game *A* is average new and has the solution value of the game v and the optimal vectors of mixed strategies of the parties

$$A - P^* = (P_1^*, P_2^*, ..., P_3^*, ..., P_n^*)$$

and

$$B - Q^* = (Q_1^*, Q_2^*, ..., Q_j^*, ..., Q_m^*)$$

during the time of the game *T* there is no aftereffect, and the sets *I*, *J* are unchanged.

The method was designed for adaptive changes of parameters and operating modes of the SS according to the game algorithm, depending on the availability of a priori information about the system settings of the offender and strategies for the creation of its attacks on information system (IS) [19].

The essence of the game control algorithm is to compare a large number of possible in these conditions qualitatively different solutions, determining the optimal or best with all the limitations solution and the formation of the corresponding team.

To improve the efficiency in solving the dynamic games the forecasting method is used.

One of the possible solutions for games in mixed strategies is, as noted above, the increase in the reaction rate (rate of adaptation) of one of the parties, which improves the efficiency of the strategies.

A common method of solving a matrix game in mixed strategies, i.e., methods of linear programming becomes much more complicated for matrixes of large dimension. The usage of decomposition methods is not always possible, and iterative solution methods, such as the method of Brown-Robinson, often have a high enough rate of convergence. As an alternative, one can use the method of dynamic programming using the results of short-term and long-term forecasting [20].

Let's take a look at the algorithm for solving matrix games using dynamic programming. In respect of cases examined long-term forecasting allows with a fairly high degree of reliability to limit the number of possible strategies for the system of the offender and reduce the game matrix. The solution of matrix games in keeping with the principle of forecasting based on the Markov approach is to optimize the conditional strategy of SS for *N* cycles forward through the predictable strategy of the intruder's system. It is obvious that with increasing *N*, the accuracy of the prediction decreases. In this regard, consider the case when $N = 1$. It is possible to allocate three stages of the algorithm for forming the optimal strategy of the SS.

The system diagram of the game management of the security system is shown in Fig. 1.

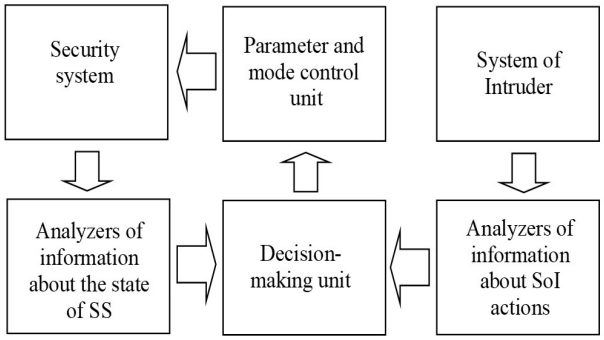

Figure 1: The system of game management (diagram)

The method of security system management based on the methods of game theory, a block diagram of the algorithm implementation consist of the following stages (Fig. 2).

The initial data input. You enter the parameters of security measures and channel decision-making $\Psi = \{\psi_i\}$, and the value of the permissible probability of incorrect decision $P_{er\,per}$.

Obtaining information about the actions of the offender's system. Using one of the methods of monitoring the status of the security system we can determine the strategy or recognize the fact of the system exposure by the intruder.

Determining the version number of the current strategy of the SS. Based on the parameters obtained in the design phase of SS, the initial strategy of the SS according to the characteristics of the remedies is determined.

Determination of the optimal strategy of SS. The problem of optimization of functioning algorithms of the SS is to determine an optimal strategy $\grave{a}^* \in \grave{A}^*$, which provides the maximum efficiency of functioning of SS within the required time functioning. To improve the efficiency in solving dynamic games the forecasting method is used.

One of the possible solutions for games in mixed strategies is, as noted above, the increase in the reaction rate (rate of adaptation) of one of the parties, which improves the efficiency of the strategies.

The adoption rate of the SS depends on the ratio T_{SS} / T_{SoI} and the value T_{SS}, T_{SoI} —from the durations of time regulation and change operating modes of protection, which depend on their position at the previous cycle. The duration of the transition of SS from the state of H_n to the state of H_m on regulation stages (H_n and H_m are the vectors of state remedies) is known in advance by a square transit time matrix of any possible (taken from the definition field) state toanother possible one:

$$\left|R_{(reg)nm}\right| N \times M,\ n = \overline{1, N},\ m = \overline{1, M}.$$

The elements of a matrix will be $T_{SS\,nm}^{reg}$ included in the T_{SS}^{H} at the stage of regulation parameters, changing modes of operation of the system. Then the process of transition from H_n to H_m, taking into account possible intermediate states can be described by a unit of homogeneous Markov chains with discrete states in discrete time. The transition from $H_n(t)$ to $H_m(t+1)$ is an appropriate strategy $a_i \in S_{SS}$. The same offender's system status in the transition is defined as $H_{PSn}(t)$ and $H_{PSm}(t+1)$.

Therefore, the task of conditional optimization of time of adaptation on the phase of adjustment consists of choosing such a strategy a^* at cycle (t+1), in which:

$$\begin{cases} T_{SS}((t+1), a^*) = \min\limits_{a_i \in S_{SS}} T_{SS}(H_n(t), \\ H_m(t+1), a_i); \\ T_{SS}((t+2), a^*) = \max\limits_{a_i \in S_{SS}} T_{SS}(H_{SSn}(t+1), \\ H_{SSm}(t+2), a_i) \end{cases}$$

considering that $T_{SS} < T_{PS}$ this happens in the process of the game solving through the introduction of k_a in the calculation of the matrix elements.

The numerical accuracy of the intended value of a win function is set to some ratio of the prediction error

$$k_{pr}(t+1|t) = \frac{\hat{\Phi}(t+1)}{\Phi_{RL}(t+1)},$$

where $\Phi_{RL}(t+1)$ is calculated when reaching (t+1) as a result of monitoring. *So*, in the case of an unchanged SoI strategy with $\Phi(t)$ for several cycles, the correction is $\Phi(t+1)$ due to $k_{pr}(t+1|t)$ that is a part of the coefficient $\beta_m(t+1)$. This eliminates a systematic error in the calculation of the values of $\Phi(t)$ and somehow influences the choice of $a^*(t+1)$ while solving matrix games.

Since the coefficient prediction error is inverse to the factor of awareness k_{inf}^{a}, the function is $f(k_{inf}^{a}) = \left|k_{pr}(t+1|t) - 1\right|$. In this case, we have the following problem of conditional optimization: $k_{inf}^{\dot{a}} \to \max$, where $\max k_{inf}^{\dot{a}} = k_{inf}^{S}$ with the limitation:

$$\left|k_{pr}(t+1|t) - 1\right| \le \delta_{er},$$

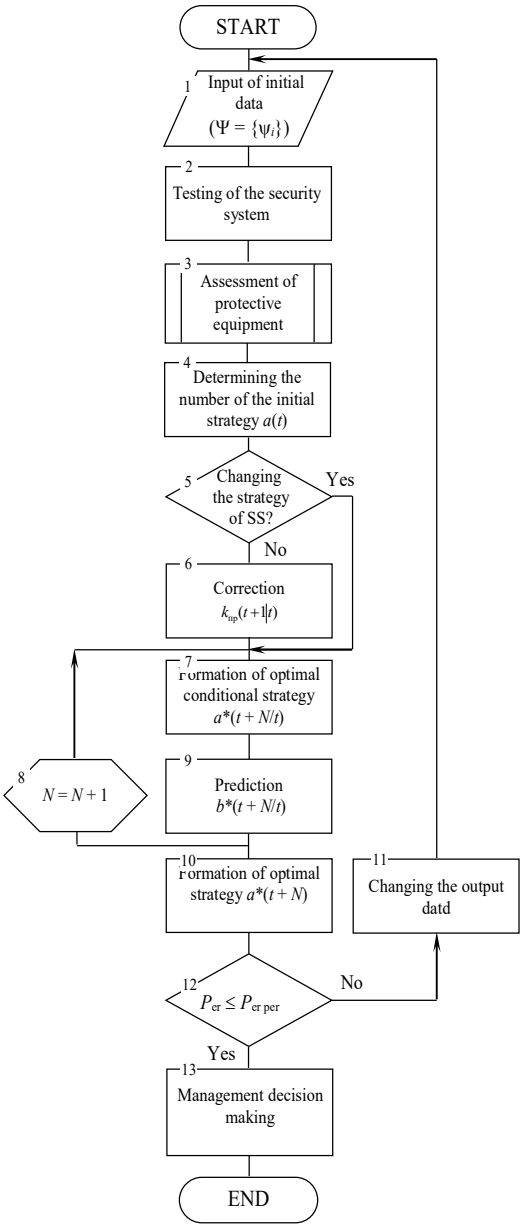

Figure 2: The block diagram of the algorithm of the methods to control security based on the model of game management

where δ_{er} is some centered random variable with zero mathematical expectation and variance δ^2, which defines some limit value of the error.

Consider the algorithm for solving matrix games using dynamic programming. In respect of cases examined long-term forecasting allows with a fairly high degree of reliability to limit the number of possible strategies for the system of the offender in the next management cycles up to 2...4 and to reduce the game matrix. The solution of the matrix game in keeping with the principle of forecasting based on the Markov approach is to optimize the conditional strategy of the SS for N cycles forward through the predictable strategy of the system of the intruder. It is obvious that with increasing N, the accuracy of the prediction decreases. In this regard, consider the case when N = 1. It is possible to allocate three stages of the algorithm for forming the SS optimal strategy. In the first phase based

on information about the current state of protection, the assumed value of the transition probabilities of *SS*, which applies to the management cycle t of the strategy system of the intruder b(t), and taking into account previous SS policies an optimal conditional strategy $\grave{a}^*(t+1|)t$ is provided:

$$a^*(t+1|)t = \arg\left[\max_{a\in S_{SS}} P(a(t), b(t), H(t))\right].$$

The second stage solves the problem of prediction strategy that is used at the management cycle *t*+1 of the SoI and which will ensure the minimization of the functional

$$b^*(t+1|)t = \arg\left[\min_{b\in S_{REP}} P(a^*(t+1), b(t+1))\right].$$

In the third stage, the optimal strategy of SS management taking into account the projected system strategy of the offender and the current status of protection measures:

$$a^*(t+1|t) = \arg\begin{bmatrix} \max\limits_{a\in S_{SS}} P(a(t+1), \\ b^*(t+1|t), \\ H(t+1), \\ \beta_m(t+1), \\ k_a(H(t+1)|H(t)) \end{bmatrix}.$$

To improve the reliability of the result the algorithm may be repeated a limited number of times if there is a certain dispersion of the probability distribution of the use of strategies $\grave{a}_1^*(t+1|t)\ldots\grave{a}_n^*(t+1|t)$ and their subsequent evaluation based on the criteria of the benefits that are introduced. In case of impossibility of definition of such a strategy $a^*(t+1)$, in which the losses do not exceed the allowable values, the problem of expanding the set of the admissible SS strategies is solved, then again, $a^*(t+1)$ is defined. Similarly, the SS strategy through conditional optimization of the management strategy of the SS for *N* steps predicted strategy of SoI is formed. The third stage of the algorithm in this case will look like this:

$$a^{*(N)}(t+N) = \arg[\max_{a\in S_{SS}} P(a(t+N), b^*(t+N|t+N-1), H(t+N), \beta_m(t+N), k_a(H(t+N)|H(t+N-1))], \quad N = 2, 3\ldots$$

The Markov chains are used at the second and third stages, which allows to calculation of the probability of a particular strategy for the next cycle of management and choice of the optimal strategy.

Let's assume that in the management cycle *t* the strategy of violator b_2 is used. Let's say, the criterium $\max\limits_{\grave{a}_1} P_{i,2}(t) = P_{3,2}$ selects the strategy a_3 (see Table 1).

Simultaneously, the prediction algorithm is implemented. Table 1 shows a simplified example of the predicted transition of the system from the state at cycle t to the state (*t*+1) based on inhomogeneous Markov chains. According to the principle of optimality, when finding the optimal solution in a multistage problem optimizing the choice of management strategy *a(t)* at each step regardless of the initial state should be aimed at optimizing not only this but also all subsequent steps. Considering the prediction for (*t*+*N*) steps forward (in this case, no more than three steps) the mechanism of choosing the optimal strategy *a*(t)* at cycle *t* will also be defined by calculating the inverse function of Bellman of the last predicted *N*–*t*+1 management cycles. *So*, for *t* = *N*:

$$B_N(H(N-1)) = \max_{a(N)\in\Lambda_N^I(H(N-1))} P_N(H(N-1), a(N)),$$

where *H*(*N*–1) is SS condition at (*N*–1)-th management cycle; *a(N)* is management strategy at a cycle of *N*; $\Lambda_N(\acute{I}\ (N-1))$ is a finite set of admissible strategies at cycle $(N-1)$.

The method of Bellman is used to improve forecast accuracy, the validity of the choice of current strategies, and decision-making support by the management device of the security system.

Table 1

The algorithm of SS predicted state transition

t	The process of prediction					*t*+1
1-st stage	2-nd stage			3-rd stage		
Decision on cycle	Probability of transition $P_{3j} = 1 - k_N\Phi_{3j}$	$\min\limits_{b_j}(1-P_{3j}(t+1))$		Probability of transition $P_{i4} = k_N\Phi_{i4}$	$\max\limits_{a_1} P_{i2}(t+1)$	
a_3	P_{31} ⇒	b_1	b_4	P_{14} ⇒	a_1	a_{12}
	P_{32} ⇒	b_2		P_{24} ⇒	a_2	
	P_{33} ⇒	b_3		P_{34} ⇒	a_3	
	P_{34} ⇒	b_4		P_{44} ⇒	a_4	
	...	...		...	...	
	P_{3j} ⇒	a_j		P_{i4} ⇒	a_{i4}	
a_3; b_2						a_2; b_4

3. Conclusions

Thus, it is worth noting some peculiarities of using this methodology, which is based on game theory about information security systems.

First of all, the winnings of the players in the mixed situation were determined to be equal to the mathematical expectation of their winnings. This assumes that the players are risk-neutral when the game situation is repeated many times. However, this is not entirely justified when considering defense systems. If an attacker can be considered a risk-neutral player, then the side of the defense is likely irrelevant. Even a one-time breach of the security of a protected system can be critical for it, putting it out of commission for a long time.

Second, the model can use certain data as input parameters. In this case, the possibilities of obtaining different data may be tasks of varying degrees of complexity. For example, if the model uses characteristics of threats, defenses, vulnerabilities, barriers, etc. as input parameters, it is quite difficult to evaluate all these characteristics and determine the relationships between them, which will complicate the practical application of the model in an intrusion detection system.

Furthermore, it is known that a large number of evaluation parameters play a very important role in detecting network intrusions. Therefore, in anomaly detection, one of the main tasks is to select the optimal set of evaluation parameters, which cannot be done using game theory methods. Therefore, it is advisable to use various mathematical methods when building security systems, in particular, intrusion detection systems.

In general, the mathematical apparatus of game theory allows for the analysis of tasks with an antagonistic, repetitive nature, which is typical for information security tasks. The proposed methods make it possible to choose at the initial stage the strategy of actions in the process of operation of the intrusion detection system and reduce the computational costs of data processing in the information security system.

Thus, in the process of constrained optimization with the current game matrix, the conventionally optimal strategy will be formed, defining the phase trajectory of the SS, starting from the final cycle of forecasting $t = N$ to the current value of t.

The main problems with the use of game theory arise in the definition of the function of gain for a particular situation. For tasks that are solved by the security system, the feature of win, first and foremost, needs to reflect the change in the security system.

If this situation is not satisfied with the SS, we should implement measures to increase winnings with certain combinations of modes.

If the attacker deviates from its optimal strategy, the SS has the opportunity to increase its winnings by deviating from the optimal strategy as well.

The results of simulation modeling of the SS functioning process on the proposed game algorithm showed that the additional use of forecasting strategies at N cycles ahead allows to improve the efficiency by 5–8%.

Thus, the theory of games allows us to offer recommendations for creating the management strategy for the operation of the protection systems. And, at least for certain types of conflicts and matrixes of winnings, these recommendations allow SS to win and improve their technical characteristics.

Analysis of winning, which gets SS in different situations showed that game theory not only allows us to generate an optimal strategy that can guarantee a certain win but also allows you to issue recommendations for its switching to increase the winnings if the system of the violator deviates from his optimal strategy. When the system of the offender follows his optimal strategy, game theory allows to evaluation of the situation. If evaluation results are not satisfied, it is necessary to implement measures to change the situation.

References

[1] P. Anakhov, et al., Protecting Objects of Critical Information Infrastructure from Wartime Cyber Attacks by Decentralizing the Telecommunications Network, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3050 (2023) 240-245.

[2] V. Zhebka, et al., Optimization of Machine Learning Method to Improve the Management Efficiency of Heterogeneous Telecommunication Network, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 3288 (2022) 149–155.

[3] S. Toliupa, et al., An Approach to Restore the Proper Functioning of Embedded Systems Due to Cyber Threats, in: Information Technology and Implementation (IT&I-2023), vol. 3624 (2023) 301–316.

[4] V. Kazimko, Application of Game Theory for Modeling Information Security Problems, Telecommun. Inf. Technol. 1(74) (2022) 123–134. doi: 10.31673/2412-4338.2022.011524.

[5] C. T. Do, er al., Game Theory for Cyber Security and Privacy, ACM Computing Surveys (CSUR), 50(2) (2017).

[6] R. Hryshchuk, Theoretical Foundations of Modeling of Information Attack Processes using the Methods of Theories of Differential Games and Differential Transformations: Monograph (2010).

[7] D. Bauso. Game Theory: Models, Numerical Methods and Applications, Foundations and Trends in Systems and Control, 1(4) (2014) 379–522.

[8] T. Nguyen, et al. Multistage Attack Graph Security Games: Heuristic Strategies, with Empirical GameTheoretic Analysis. Security and Communication Networks (2018). doi: 10.1155/2018/2864873.

[9] S. Roy, et al., A Survey of Game Theory as Applied to Network Security, in: 43rd Hawaii International Conference on System Sciences (2010) 1–10.

[10] R. Sankardas, et al., A Survey of Game Theory as Applied to Network Security, Hawaii International Conference on System Sciences (2010).

[11] V. Kazimko, Application of Game Theory for Modeling Information Security Problems, Telecommun. Inf. Technol. 1(74) (2022). doi: 10.31673/2412-4338.2022.011524.

[12] D. Akinwumi, et al., A Review of Game Theory Approach to Cyber Security Risk Management, Nigerian J. Technol. 36(4) (2017). doi: 10.4314/njt.v36i4.38.
[13] E. Borel, La théorie du jeu les équations integrales á yau symétrique. Comptes Rendus de l'Académie, 173 (1921) 1304–1308.
[14] S. Shevchenko, et al., Protection of Information in Telecommunication Medical Systems based on a Risk-Oriented Approach, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3421 (2023) 158–167.
[15] S. Shevchenko, et al., Conflict Analysis in the "Subject-to-Subject" Security System, Cybersecurity Providing in Information and Telecommunication Systems Vol. 3421 (2023) 56–66.
[16] S. Shevchenko, et al., Conflicting Subsystems in the Information Space: A Study at the Software and Hardware Levels, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 3654 (2024) 333–342.
[17] V. Astapenya, et al., Conflict Model of Radio Engineering Systems under the Threat of Electronic Warfare, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 3654 (2024) 290–300.
[18] S. Toliupa, T. Babenko, A. Trush, The Building of a Security Strategy based on the Model of Game Management, in: 4th International Scientific-Practical Conference Problems of Infocommunications Science and Technology, PIC S and T 2017 – Proceedings (2017) 57–60.
[19] S. Huang, et al., Markov Differential Game for Network Defense Decision-Making Method, IEEE Access, 6 (2018) 39621–39634.
[20] T. Nguyen, et al., Multistage Attack Graph Security Games: Heuristic Strategies, with Empirical GameTheoretic Analysis, Security and Communication Networks (2018). doi: 10.1155/2018/2864873.