I.J. Intelligent Systems and Applications, **2017, 12, 46-58**
Published Online December 2017 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijisa.2017.12.05

Method for Optimization of Information Security Systems Behavior under Conditions of Influences

Zhengbing Hu
Central China Normal University, Wuhan, China
E-mail: hzb@mail.ccnu.edu.cn

Yulia Khokhlachova and Viktoriia Sydorenko
Department of Information Technology Security, National Aviation University, Kyiv, Ukraine
E-mail: hohlachova@gmail.com, v.sydorenko@ukr.net

Ivan Opirskyy
Department of Information Security, National University "Lviv Polytechnic", Lviv, Ukraine
E-mail: iopirsky@gmail.com

Received: 04 June 2017; Accepted: 11 September 2017; Published: 08 December 2017

Abstract—The paper analyzes modern methods of modeling impacts on information systems, which made it possible to determine the most effective approaches and use them to optimize the parameters of security systems. And also as a method to optimize data security, taking in the security settings account (number of security measures, the type of security subsystems, safety resources and total cost information) allows to determine the optimal behavior in the "impact-security". Also developed special software that allowed to verify the proposed method.

Index Terms—Information Security, Information Security Systems, Information Influence, Information Systems Jptimization, Modeling Impacts.

I. Introduction

The development of modern informative and communicative technologies influences on all spheres of human activity, rising their effectiveness, and simultaneously causing a set of uncontrolled threats, also including in informational sphere. Due to this, requirements for security of crucial important informational resources rise constantly. Today, key and crucial international laws in informational security (hereinafter referred to as "ISec") management sphere and information security are series of standards ISO 27k. According to them, the main procedures for organization an effective system of ISec management are resources management, communication and operation management, risks management, work persistence management, ISec incidents management etc. Incidents management, according to international standard ISO/IEC 27035:2011, allows to reveal, analyze and investigate effectively, and in proper time, ISec incidents for minimization negative consequences for informational systems (hereinafter referred to as "IS") and organizations in general. Besides mentioned international standard, today there are many trade laws, and also practical recommendations and guides, that are based on the best world incident-management practices. According to these documents, carrying out a procedure of incidents management is entrusted to specialized groups of fast reaction, which according to their functional peculiarities, provide for their clients certain services. Among basic services, should be mentioned identification and incidents analysis, reaction to incidents and their investigation, IS threats analysis, and also examining their endurance by simulation of attacks and impacts. Taking into consideration that success of realization of informational impact on the system, depends on its vulnerabilities, and in worse case turns into an incident, the investigation of system behavior under the influence of informational impacts, from the point of information security, is actual area for scientific research.

II. Related Works

Let's review modern approaches to modeling of impacts on IS, we will mention input and output data of every criterion, main operations and also their advantages and drawbacks [1-3,5,8] (Table 1). The carried out research of modern methods of impacts simulation on informational systems has provided a possibility to define the most effective approaches (they are marked using grey color in the table 1) and to use them in order to optimize parameters of security systems. Taking into consideration the carried out research, today many tasks have left, and the task of solving them, have scientific and practical value. From this point of view, the designing and research of optimization methods of security systems indicators under conditions of influences are actual scientific task. Taking into

consideration this point, the purpose of this work is designing a method of optimization of information security systems behavior under conditions of informational influences.

Table 1. Analysis of methods of impacts modeling on IS

No.	Name	Input data	Output data	Main operations (mathematical tool)	Advantages	Drawbacks
1.	The Mukchin-Volokita model [8]	Statistical data selection	Calculation of threats impacts on information	Expert estimations, graph theory	High accuracy of impact detection	A need of statistical data, dependence on competence of experts
2.	The Bell–LaPadula model and Biba model [8]	Sets of objects and subjects, and also their states, requests	A level of integrity breach	Sets theory, Boolean algebra	Simplicity of realization, integrity control	Taking into account only integrity; a possibility of creating of two-way information flow, and as a result is necessary to create trustful flows
3.	The Hartson model (five-dimensional model) [6]	Resources and their states; users and their responsibilities	A sphere of system security	A Cartesian product	A possibility of obtaining quantitative values	Abstract formalization of attack process
4.	A model on base of neuron Markov chains [3]	Statistical data for learning neuron networks, and specifying matrixes of probabilities conversions of Information Security System (ISS)	Identifying viruses, spam and attacks on Web-services	A theory of neuron networks; Markov's chains theory	Adaptive identifications of attack and information security	A need for statistical data set for dynamical functioning
5.	A model on base of Petri-Markov networks [1]	Informational states of system (more then 3)	A possibility of realization of threats impact on information	Petri network theory and Markov chains theory	Quantitative estimation with taking into consideration time parameters	Difficulties of calculations for practical realization
6.	Differential gaming one-criterion column model [3]	The set of IS states	Optimal strategy of information security	A column theory, differential-gaming simulation	It allows to carry out distribution of informational resources, that are assigned to informational security	It doesn't show general dynamics of influence on information
7.	Differential-gaming spectral one-criterion models [3]	The set of IS states	Optimal strategy and price of the game (guaranteed level of security)	Differential-gaming simulation	Low calculating difficulty, taking into account non-stationary processes	Not accurate step-by-step process of influence on information
8.	Differential-gaming Teylor model [3]	Flow intensity of protective and attacking actions	Trajectory and price of the game	Differential conversions of Teylor type	Accurate description of attack on information	High calculating difficulty, low level of scientific-technical researches
9.	Hybrid differential-gaming model [3]	Reliability and security indicators, threats probability, time parameters	Optimal distribution of security resources	Differential-gaming simulation	Taking into account an indicator of ISS qualitative functioning; high accuracy even in uncertain cases	Accuracy is reached only with using certain mathematical methods (consecutively)
10.	Constant discrete differential-gaming model [3]	Ultimate set of system state	Optimal security resources distribution in real time	Numeral-analytical simulation, differential conversions	Extension of simulation range of impact on information, low calculating difficulty	It doesn't take into consideration all criteria (comparing with multi-criteria models)
11.	Multi-criteria differential-gaming model on base of integral optimality [3]	Strategies of opposing parties, time parameters	Optimal players strategies, price of the game (guaranteed security level)	Differential-gaming simulation, a theory of decision making	A possibility of information security under condition of conflict of partial criteria, and unauthorized distribution of informational resources of attacking party	Limitations on partial criteria of quality
12.	Multi-criteria differential-gaming model on base of non-linear scheme of compromises [2,3]	Intensity of resources distribution flow of opposing parties, time characteristics	Optimal strategies of opposing parties	Differential conversions, a theory of support of decision making	Realization simplicity, adaptability to different situations	Notable drawbacks haven't been found

III. Theoretical Basis of Optimization Methods of Security Systems Indicators under Conditions of Influences

A typical task of ISS behavior research under conditions of influences on information, is optimal resources distribution of player of security in correspondence with player of influence. Let suppose two systems. One of the system is system of influence (SI) is a player, that influences on information of another system (Information security system, hereinafter referred to as "ISS"), a player, that ensures security.

To carry out this task, SI uses certain amount of methods and influential means. The influential means of SI consist of S_1 types, and they are in certain conventional units, quantity of means of m-th type is equal to a_m. The total attacking potential of SI M_1 is a value, that is equal to $M_1 = \sum_{m=1}^{S_1} a_m$.

The information that should be protected, has n informational blocks $B_i,...,B_n$, besides the value of B_i-th block is evaluated by certain conditional value v_i, where $i = 1,...,n$. Let mention that the informational blocks $B_i,...,B_n$, are sorted by their value, i.e. $v_i \geq \cdots \geq v_n$.

Let suppose that every unprotected informational block B_i during influence on information and realization of single influence using means of m-th type, loses its characteristics – integrity, availability and confidence. The value of losses from influence on information in ISS on B_i-th informational block is evaluated by value $v_i \varepsilon_m$.

The total losses of integrity, availability and confidence of information $I(\lambda, \mu)$, which define its security in ISS, only if availability of influences and opposition can be evaluated by value, proportional to difference of their total quantity, if it is positively defined, and equal to zero in opposite case, i.e.

$$I(\lambda, \mu) = \sum_{i=1}^{n} v_i \max\left\{0, \sum_{m=1}^{S_1} \varepsilon_m \left(\mu_{im} - \sum_{j=1}^{S_2} \lambda_{mj} \lambda_{ij} \right)\right\} \quad (1)$$

where μ_{im} is an intensity of flow of informational influences, that are assigned by SI to influence on B_i-th informational block using means of influence of m-th type;

λ_{ij} is an intensity of flow of actions, that are assigned by ISS for ensuring security of B_i-th informational block using means of ensuring security of j-th type;

λ_{mj} is an intensity of flow of actions, that are assigned by ISS for preventing influence from means of m-th type, using means of ensuring security of j-th type.

The distribution of means of ensuring security of j-th type, that are assigned by ISS for preventing influence from means of m-th type on condition that $\sum_{m=1}^{S_1} \lambda_{mj} = 1$, $1 \leq j \leq S_2$ and $1 \leq m \leq S_1$, can be showed in matrix view:

$$\Lambda = \left\| \lambda_{mj} \right\| \quad (2)$$

using correspondence limitations

$$0 \leq \lambda_{mj} \leq \lambda_{mj\max} \quad (3)$$

where $\lambda_{mj\max}$ is maximum intensity of flow of actions, considering ensuring security $\lambda_{mj\max} = 1$.

Let the total value of losses of information in ISS $I(\lambda, \mu)$ (1) be the main characteristic of informational conflict, and its source is opposition of interests of ISS and SI. However, ISS tries to improve the information security by reducing the value of total losses (1), that are caused by actions of SI's influences. The goal of SI is the opposite, that's why the function (1) can be accepted as a fee of information security ensuring system for SI. As a result, the task of synthesis of optimal behavior in the system "security-influence" comes to antagonistic game of two players with convex function by one variable λ and function of win $I(\lambda, \mu)$ (1), when the second variable μ has arbitrary fixed value.

Proceeding from a methodology of finding the solutions of antagonistic games for convex function by one variable of function of win [2,4,7], let's form a task of synthesis of optimal behavior in "security-influence" system in view of the following a theorem.

A. Theorem 1

Let a fee $I(\lambda, \mu)$ be persistent function of win with two variables λ and μ for antagonistic game, which is strictly convex by λ for each arbitrary fixed μ, and has on single range first derivative by λ. Then only one optimal protective strategy exists for ISS λ^{opt}, that is stepped function of fee $I(\lambda^{opt}, \mu)$, and $\lambda^{opt} = const$, and the only answer of equation is

$$I(\lambda^{opt}, \mu) = \max_{0 \leq \mu \leq 1} I(\lambda^{opt}, \mu) \quad (4)$$

If two players – SI and ISS have chosen the optimal strategies μ^{opt} and λ^{opt}, then the price of the game I^* can be defined as

$$I^* = \min_{0 \leq \lambda \leq 1} \max_{0 \leq \mu \leq 1} I\left(\lambda^{opt}, \mu^{opt}\right) \quad (5)$$

B. Proof

Optimal strategy of player of influence μ^{opt} can be defined depending on value of optimal strategy of player

who ensures security λ^{opt}. If the player, who ensures security, chooses one of the optimal strategy:

$$\lambda^{opt} = \begin{cases} 1, \dfrac{\partial I\left(\lambda^{opt}, \mu^{opt}\right)}{\partial \lambda} \le 0; \\ 0, \dfrac{\partial I\left(\lambda^{opt}, \mu^{opt}\right)}{\partial \lambda} > 0, \end{cases} \tag{6}$$

then player of influence will choose the following strategy $\mu^{opt} = const$, that will satisfy the conditions

$$0 \le \mu^{opt} \le 1 \tag{7}$$

and expression (5).

If the player who ensures security evades sticking to the optimal strategy λ^{opt} in range $0 < \lambda < 1$, then the player of influence will choose the strategy like

$$\mu(\alpha) = \alpha I(\lambda, \mu_1) + (1-\alpha) I(\lambda, \mu_2) \tag{8}$$

where α, μ_1, μ_2 are arbitrary constants, that meet the conditions

$$\begin{gathered} 0 < \alpha < 1,\ 0 < \mu_1 < 1,\ 0 < \mu_2 < 1 \\ I\left(\lambda^{opt}, \mu_1\right) = I\left(\lambda^{opt}, \mu_2\right) = I,\ \frac{\partial I\left(\lambda^{opt}, \mu_1\right)}{\partial \lambda} \ge 0, \\ \frac{\partial I\left(\lambda^{opt}, \mu_2\right)}{\partial \lambda} \le 0,\ \alpha \frac{\partial I\left(\lambda^{opt}, \mu_1\right)}{\partial \lambda} + (1-\alpha) \frac{\partial I\left(\lambda^{opt}, \mu_2\right)}{\partial \lambda} = 0 \end{gathered} \tag{9}$$

C. Note

Used requirements in function of fee $I(\lambda, \mu)$ (1) can be weakened.

First, it is possible to neglect the conditions of existing the derivatives. But in this case, is supposed the existing of single sided derivative functions $I(\lambda, \mu)$ at every point of interval of its defining. Then the conditions, that are put on the derivatives $\frac{\partial I\left(\lambda^{opt}, \mu_1\right)}{\partial \lambda}$ and $\frac{\partial I\left(\lambda^{opt}, \mu_2\right)}{\partial \lambda}$, are interchanged by corresponding conditions for single sided derivatives at the indicated points.

Second, the condition of strict convex of function of win $I(\lambda, \mu)$ is possible to weaken, by interchanging it by condition, that it is convex. But it leads to situation, that optimal strategies as for the first μ^{opt}, and as for the second λ^{opt} player, are not the only.

On base of theorem 1 and taking into consideration the note, the optimal strategy for ensuring security of ISS λ^{opt} can defined from equation

$$\inf_{\lambda} \sup_{\mu} I(\lambda, \mu) = \sup_{\mu} I\left(\lambda^{opt}, \mu\right) = I \tag{10}$$

Taking into consideration the equation (10), SI chooses mixed optimal strategy $\mu^*(\alpha)$, that is certain convex combination of finite quantity of pure strategies.

Let's bring in some designations. Let $X_i = \left\|\mu_{i1}, \ldots, \mu_{iS_1}\right\|$, $Y_i = \left\|\lambda_{i1}, \ldots, \lambda_{iS_2}\right\|$, $\zeta_i = \left\|\nu_i \varepsilon_1, \ldots, \nu_i \varepsilon_{S_1}\right\|$. Then the fee (10) with considering accepted designations can be showed in matrix view:

$$I(\lambda, \mu) = \sum_{i=1}^{n} \max\left\{0, \zeta'\left(X_i - \Lambda Y_i\right)\right\} \tag{11}$$

where ζ' is transposed matrix to matrix ζ.

Due to the reason, that function of fee $I(\lambda, \mu)$ (1) is convex by λ for every arbitrary fixed μ, then SI during forming the optimal strategy μ^{opt} can use randomized strategy only among those pure strategies, that are the tops of simplex:

$$\mu^{opt} = \left\{ \sum_{i=1}^{S_1} \delta_i \alpha_i \right\} \tag{12}$$

where $\delta_i \ge 0$, $\sum_{i=1}^{S_i} \delta_i = 1$.

And the fee (1) with considering (12) acquires the following view

$$I(\lambda, \mu) = I\left(\lambda, \sum_{i=1}^{S_1} \delta_i \alpha_i\right) \le \sum_{i=1}^{S_1} \delta_i I(\lambda, \alpha_i) \tag{13}$$

Let's mark by I_m a part of price of the game I^*, which can be obtained by SI on account of using the means of influence of m-th type, that $\sum_{m=1}^{S_1} I_m = I^*$ and $Q = \left\|a_1, \ldots, a_{S_1}\right\|$. Then, for defining the strategy of ensuring security of B_i-th informational block for ISS, according to stated theorem no. 1, we obtain the matrix equation

$$Q - \Lambda Y_i = I_i \tag{14}$$

To solve this matrix equation (14) is worth using generalized inverse matrix of Moore–Penrose, first time implemented in work [9].

Let for rectangular matrix Λ [9] exist generalized inverse matrix of Moore–Penrose Λ^+, for which the following conditions are true [9]:

$$\begin{gathered} \Lambda\Lambda^+\Lambda = \Lambda,\ \Lambda^+\Lambda\Lambda^+ = \Lambda^+ \\ \left(\Lambda\Lambda^+\right)^* = \Lambda\Lambda^+,\ \left(\Lambda^+\Lambda\right)^* = \Lambda^+\Lambda \end{gathered} \tag{15}$$

where Λ^* is the conjugate transposed matrix, which for matrix Λ in range of real numbers is transposed, i.e. $\Lambda^* = \Lambda'$.

Thus, for non-particular square matrix Λ (2) is defined generalized inversed matrix Λ^+, which matches with ordinary inversed matrix Λ^{-1}, i.e. $\Lambda^+ = \Lambda^{-1} = \|\beta_{ij}\|$.

Taking into consideration the peculiarities of generalized inversed matrix (13) from matrix equation (14) we receive

$$Y_i = \Lambda^+(Q - I_i) \tag{16}$$

where the strategy of ensuring security of B_i -th informational block by means of ensuring security of j -th type of ISS λ_{ij}, that defines the intensity of actions flow considering ensuring security, with taking into account accepted above designations, acquires the view

$$\lambda_{ij} = \sum_{m=1}^{S_1} \beta_{jm}\left(a_m - \frac{I_m}{\nu_i \varepsilon_m}\right) \tag{17}$$

Let's presume, that ISS places its means of preventing of j -th type among the most valuable information $\psi(j)$, i.e.

$$\lambda_{\psi(j)+1,j} = \lambda_{\psi(j)+2,j} = \ldots = \lambda_{n,j} = 0 \tag{18}$$

Summarizing the values (17) by all n informational blocks $B_i,\ldots,B_n$ and taking into account the presumption (18), we define the strategy for player in case of ensuring security for the most valuable information:

$$\sum_{i=1}^{\psi(j)} \lambda_{ij} = \psi(j)\sum_{m=1}^{S_1} \beta_{jm} a_m - L_{\psi(j)} \sum_{m=1}^{S_1} \beta_{jm} \frac{I_m}{\varepsilon_m} \tag{19}$$

where $L_{\psi(j)} = \sum_{i=1}^{\psi(j)} \frac{1}{\nu_i}$.

As $\sum_{i=1}^{\psi(j)} \lambda_{ij} = d_j$, according to presumption, and taking into consideration (19), we have

$$\sum_{m=1}^{S_1} \beta_{jm} \frac{I_m}{\varepsilon_m} = \frac{1}{L_{\psi(j)}}\left[\psi(j)\sum_{m=1}^{S_1} \beta_{jm} a_m - d_j\right] \tag{20}$$

Let's designate $S = \left\| \begin{matrix} \frac{\psi(1)}{L_{\psi(1)}} & 0 & \ldots & 0 \\ & \frac{\psi(2)}{L_{\psi(2)}} & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & \frac{\psi(S_2)}{L_{\psi(S_2)}} \end{matrix} \right\|$,

$$R = \left\| \frac{d_1}{\psi(1)},\ldots,\frac{d_{S_1}}{\psi(S_2)} \right\|,\ W = \left\| \frac{I_1}{\varepsilon_1},\ldots,\frac{I_{S_1}}{\varepsilon_{S_1}} \right\|$$

proceeding from accepted designations, let's go over from the equation (20) to its matrix form

$$\Lambda^+ W = S\left(\Lambda^+ Q - R\right) \tag{21}$$

After using the peculiarities of generalized inverse matrix (15) from the expression (21) after simplification, we have

$$W = \Lambda S\left(\Lambda^+ Q - R\right) \tag{22}$$

where the part of price of the game I_m, that is the fee of ISS for losses of the most valuable information, is defined as

$$I_m = \varepsilon_m \sum_{j=1}^{S_2} \frac{\lambda_{mj}}{L_{\psi(j)}}\left[\psi(j)\sum_{m=1}^{S_1} \beta_{jm} a_m - d_j\right]. \tag{23}$$

The SI will act optimally, if it influences on the most valuable information $\psi = \max\psi(j)$, which the ISS ensures security with certain probability p_i. Besides the price of the game for SI can be defined as

$$I^* = \sum_{m=1}^{S_1} I_m = \sum_{m=1}^{S_1}\sum_{j=1}^{S_2} \frac{\varepsilon_m \lambda_{mj}}{L_{\psi(j)}}\left[\psi(j)\sum_{m=1}^{S_1} \beta_{jm} a_m - d_j\right] \tag{24}$$

D. A conclusion from the theorem 1

Mathematical expectation of win by all means of influence on every block of information B_i, for which is ensured security by all means of ensuring security by ISS, doesn't depend on number of informational block i, i.e. $p_i \nu_i = c = const$. Taking into consideration the condition of settings $\sum_{i=1}^{\psi} p_i = 1$, we have $p_i = \begin{cases} c/\nu_i, 1 \le i \le \psi; \\ 0, i > \psi, \end{cases}$.

where $c = \left(\sum_{i=1}^{\psi} \frac{1}{\nu_i}\right)^{-1} = \frac{1}{L_\psi}$.

Thus, the synthesis of optimal behavior of ISS-SI, is defined by optimal strategies of the players in informational conflict, the expressions (6) and (12) correspondingly.

E. Example

Let the ISS choose arbitrary strategy for ensuring security, but it is not optimal (6), then the choice of optimal strategy (12) by SI, guarantees its win in fee E_1 not less than the price of the game I^* (24), i.e.

$$E_1 = \sum_{i=1}^{\psi} \frac{1}{\nu_i L_\psi} \sum_{m=1}^{S_1} \varepsilon_m \left[a_m - \sum_{j=1}^{S_2} \lambda_{mj} \lambda_{ij} \right] =$$

$$= \frac{\psi}{L_\psi} \varepsilon_m \left[\sum_{j=1}^{S_2} \sum_{m=1}^{S_1} \beta_{jm} a_m \lambda_{mj} \right] - \sum_{i=1}^{\psi} \frac{1}{L_\psi} \sum_{m=1}^{S_1} \varepsilon_m \sum_{j=1}^{S_2} \lambda_{mj} \lambda_{ij} \geq$$

$$\geq \sum_{m=1}^{S_1} \varepsilon_m \sum_{j=1}^{S_2} \left[\psi(j) \sum_{m=1}^{S_1} \beta_{jm} a_m \lambda_{mj} \right] \frac{1}{L_{\psi(j)}} - \sum_{m=1}^{S_1} \varepsilon_m \sum_{j=1}^{S_2} \frac{\lambda_{mj} d_j}{L_{\psi(j)}} =$$

$$= \sum_{m=1}^{S_1} \sum_{j=1}^{S_2} \frac{\varepsilon_m \lambda_{mj}}{L_{\psi(j)}} \left[\psi(j) \sum_{m=1}^{S_1} \beta_{jm} a_m - d_j \right] = I^* \qquad (25)$$

Let suppose that the strategy of influence of SI is not optimal, then proceeding from the matrix equation (11), the losses of information in ISS don't exceed the values E_2:

$$E_2 = \nu_i \sum_{m=1}^{S_1} \varepsilon_m \left\{ \mu_{im} - \sum_{j=1}^{S_2} \lambda_{mj} \left[\beta_{jm} \left(a_m - \frac{I_m}{\nu_i \varepsilon_m} \right) \right] \right\} \leq$$

$$\leq \nu_i \{ \sum_{m=1}^{S_1} \varepsilon_m [a_m - \sum_{j=1}^{S_2} \sum_{m=1}^{S_1} \beta_{jm} a_m \lambda_{mj} +$$

$$\leq \nu_i \{ \sum_{m=1}^{S_1} \varepsilon_m [a_m - \sum_{j=1}^{S_2} \sum_{m=1}^{S_1} \beta_{jm} a_m \lambda_{mj} +$$

$$= \nu_i \left\{ \sum_{m=1}^{S_1} \varepsilon_m \, a_m - \left[\sum_{m=1}^{S_1} \varepsilon_m \, a_m + \sum_{m=1}^{S_1} \frac{I_m}{\nu_i} \right] \right\} = I \qquad (26)$$

Proceeding from these ratios, is followed the truth of stated according to the theorem no. 1 expressions. Thus, the theorem n 1 has been proved.

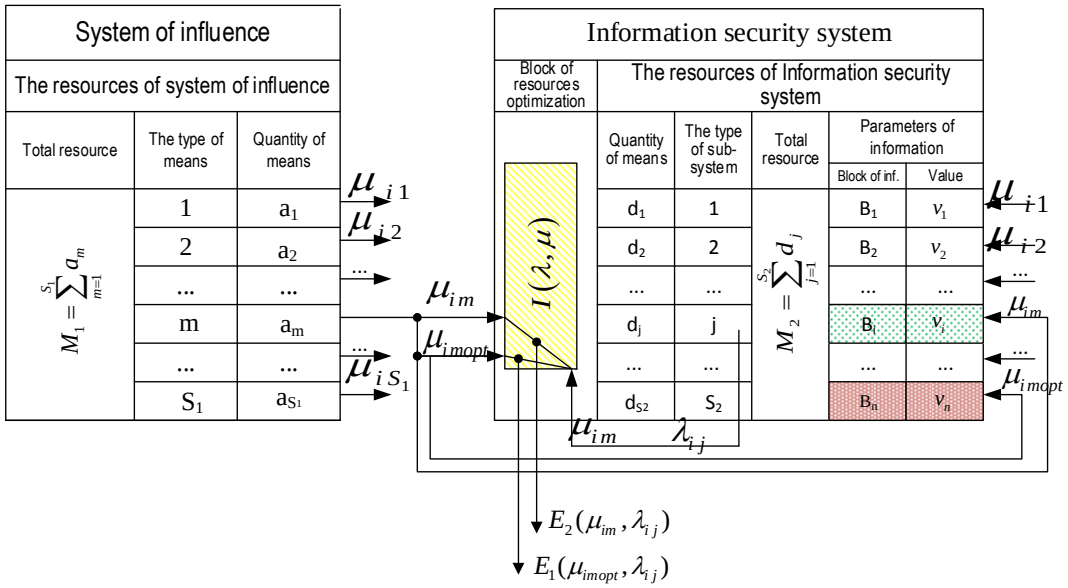

Fig.1. A scheme of representing the method of optimization of information security systems behavior under conditions of influences

The suggested method of optimization of information security systems behavior under conditions of influences is represented in fig. 1. A typical task of research of behavior of security system under the conditions of influences is optimal resources distribution of player of security, corresponding resources of player of influence.

IV. Experimental Research of Method of Optimization of Security System Indicators under Conditions of Influences

A. Estimation of predicted and current level of informational resources security for different strategies of forming system security

The task of synthesis of optimal behavior with using developed software, allows to evaluate the predicted $I(\lambda^{opt}, \mu^{opt})$ current $I(\lambda, \mu)$ levels of informational resource security, depending on strategies λ and μ, that are chosen by players – the subjects of conflict on defined interval $[t_0, T]$, where t_0 a moment of time at the beginning of informational conflict, T the time of its ending. The procedure of evaluating comes to simulation of antagonistic game of two players.

In this work is researched three strategies of forming system security [3, 12, 13]: a strategy of forming of echelon security system with n barriers of security, a strategy of withdrawal of player of influence to erroneous informational resource with further involving it in informational conflict, and a strategy of estimation of security level using a pattern of normal system behavior.

According to description of method of optimization of security system behavior under conditions of influences, the security level, depending on chosen strategies of forming such systems, in general view is defined according to (1). Besides, for different strategies of security system security, that are chosen by player of security, the predicted $I(\lambda^{opt}, \mu^{opt})$ and current $I(\lambda, \mu)$

levels of security of informational resource, acquire the values, that vary in range $I \in [0,1)$. Let's evaluate the predicted and current level of informational resources security for each of them.

The strategy of forming of echelon security system with n barriers of security is described in works [3, 5, 15]. In fig. 2 is described a graph model of attacking process (impact) on echelon security system.

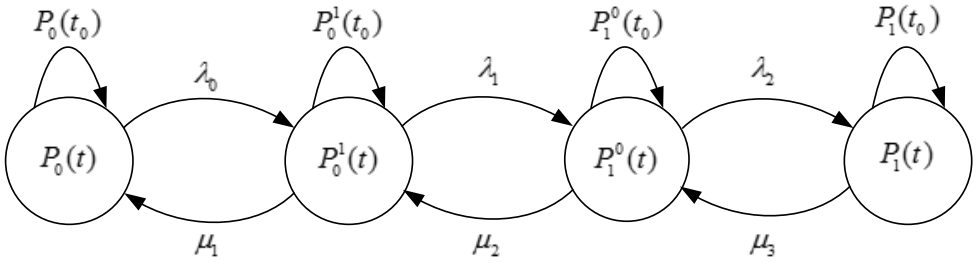

Fig.2. A graph model of attacking process (impact) on echelon security system

In fig. 2 $P_0(t)$ is a probability of stay of security system under the influence of unauthorized access (hereinafter referred to as "UA"), $P_0^1(t)$ is a probability of stay of security system under the influence of UA means during action of securitize methods, $P_1^0(t)$ is a probability of stay of security system under the influence of security during action methods of UA, $P_1(t)$ is a probability of stay of security system under the influence of security methods, $\lambda_0, \lambda_1, \lambda_2, \mu_1, \mu_2, \mu_3$ are intensities of flow of securitize actions and informational attacks under corresponding probabilities. $P_0(t_0)$, $P_0^1(t_0)$, $P_1^0(t_0)$, $P_1(t_0)$ are starting conditions for corresponding probabilities.

For this strategy in work [3, 13] was shown, that during using of echelon security system with 4 barriers of security $(n=4)$ and arbitrary strategies of security and influence, the expression of evaluation (1) acquires the view:

$$I^*(\lambda_0, \lambda_1, \mu_1)_{UA} = 1 - \frac{1}{2}\lambda_0 T + \frac{1}{6}\lambda_0(\lambda_0 + \mu_1)T^2 - \\ - \frac{1}{24}\lambda_0\left(\lambda_0^2 + 2\lambda_0\mu_1 + \lambda_1\mu_1 + \mu_1^2\right)T^3.$$

On base of shown expression and step of change of λ parameters (the intensity of securitize actions per unit of time), μ (the intensity of influences per unit of time) and time t, and using software «Optima – 2014 v.1.0», we have received the following dependences of security level (table 2).

Table 2. The security level of security system during using the echelon security system

λ	μ	T=0,2 sec	T=0,4 sec	T=0,6 sec	T=0,8 sec	T=1 sec
0,00	1,00	1,000	1,000	1,000	1,000	1,000
0,25	0,00	0,975	0,952	0,929	0,906	0,885
0,25	0,25	0,976	0,953	0,932	0,912	0,893
0,25	0,50	0,976	0,955	0,935	0,917	0,900
0,25	0,75	0,977	0,956	0,938	0,921	0,906
0,25	1,00	0,977	0,957	0,940	0,925	0,911
0,50	0,00	0,952	0,906	0,864	0,824	0,786
0,50	0,25	0,952	0,909	0,870	0,834	0,801
0,50	0,50	0,953	0,912	0,876	0,843	0,813
0,50	0,75	0,954	0,915	0,880	0,850	0,822
0,50	1,00	0,955	0,917	0,885	0,856	0,828
0,75	0,00	0,929	0,864	0,805	0,751	0,701
0,75	0,25	0,930	0,868	0,813	0,764	0,719
0,75	0,50	0,931	0,872	0,821	0,775	0,732
0,75	0,75	0,932	0,876	0,827	0,784	0,742
0,75	1,00	0,933	0,879	0,833	0,791	0,748
1,00	0,00	0,906	0,824	0,751	0,685	0,625
1,00	0,25	0,908	0,829	0,761	0,700	0,643
1,00	0,50	0,909	0,834	0,770	0,712	0,656
1,00	0,75	0,911	0,839	0,777	0,721	0,664
1,00	1,00	0,912	0,843	0,784	0,728	0,667

In fig. 3 is shown the dependence of security level $I(\lambda,\mu)$ on time t.

As it is seen from the table 2 and fig. 3, if the players have chosen the optimal strategies of security and influence correspondingly, the predicted level of informational resource security using the echelon security system will be equal to 0,667 (for $T=1\text{sec}$), i.e. $I(\lambda^{opt},\mu^{opt})=0.667$. For the rest of occurrences, when the players evade from optimal strategies, this value varies in range of specified limitations.

In fig. 4 $P_0(t)$ is a probability of stay of security system under the influence of UA, $P_0^1(t)$ is a probability of stay of security system under the influence of UA when security methods are active, $P_1^0(t)$ is a probability of stay of security system under the influence of security methods when methods of UA are active, $P_1(t)$ is a probability of stay of security system under the influence of security methods, $\lambda_0,\lambda_1,\lambda_2,\mu_1,\mu_2,\mu_3$ are the intensities of flows of security actions and informational attacks for corresponding probabilities.

For this strategy in work [3, 5, 14] was shown, that in case of arbitrary security strategies and influence the expression of evaluation (1) acquires the view:

$$I^*(\lambda_1,\lambda_2,\mu_1,\mu_2)_{UA}=1-\frac{1}{2}(\lambda_1+\lambda_2)T+$$
$$\frac{1}{6}\left((\lambda_1+\lambda_2)^2+\lambda_1\mu_1+\lambda_2\mu_2\right)T^2-\frac{1}{24}(((\lambda_1+\lambda_2)((\lambda_1+\lambda_2)^2+$$
$$+\lambda_1\mu_1+\lambda_2\mu_2+\lambda_1\mu_1(2\lambda_2+\lambda_1+\mu_1)+\lambda_2\mu_2(2\lambda_1+\lambda_2+\mu_2).$$

On base of this expression and step of change of λ parameters (the intensity of security actions per unit of time), μ (the intensity of influences per unit of time) and time t, and using software «Optima – 2014 v.1.0», we have received the following dependences of security level (table 3).

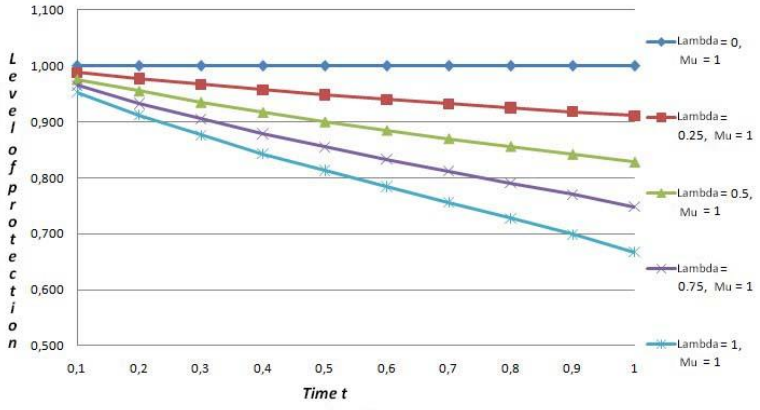

Fig.3. The dependence of security level $I(\lambda,\mu)$ on time t in case of using the echelon security system

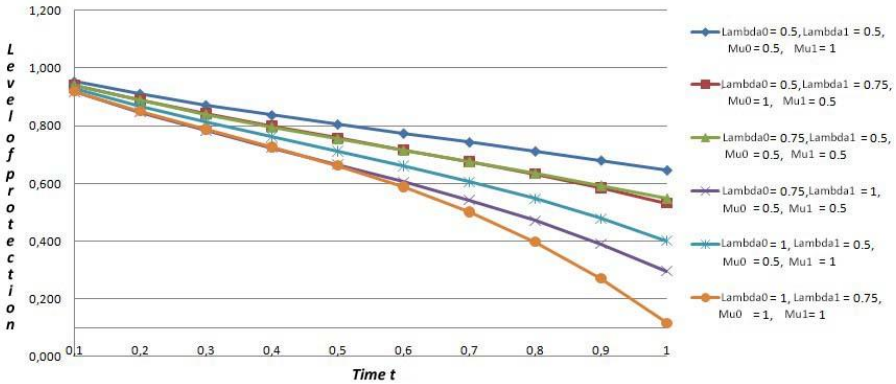

Fig.4. The dependence of security level $I(\lambda,\mu)$ on time t in case of using the strategy of withdrawal of player of influence to erroneous informational resource with further involving it in informational conflict

As it is seen from the table 3 and fig. 4, if the players have chosen the optimal strategies of security and influence correspondingly, the predicted level of informational resource security using the strategy of withdrawal of player of influence to erroneous informational resource with further involving it in informational conflict, will be equal to 0,6044 (for $T=1\text{sec}$), i.e. $I(\lambda^{opt},\mu^{opt})\approx 0.6044$. For the rest of occurrences, when the players evade from optimal strategies, this value varies in range of specified limitations.

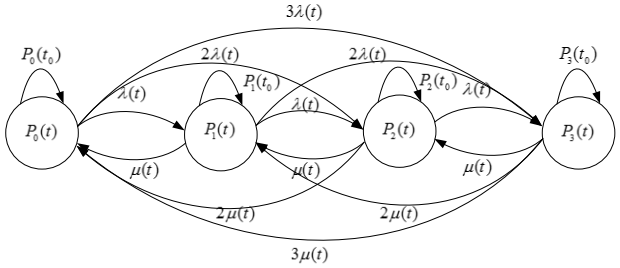

Fig.5. A graph model of process of attack on security system, that uses the strategy of estimation of security level using a pattern of normal system behavior

The strategy of estimation of security level using a pattern of normal system behavior is described in works [3, 5, 10, 16]. In fig. 5 is shown a graph model of process of influence (attack) on security system, that uses the strategy of estimation of security level using a pattern of normal system behavior.

In fig. 5 $P_0(t)$ is a probability of system failure under the influence of attack, $P_1(t)$ is a probability of stay of system under the influence of attack when information security methods are active, $P_2(t)$ is a probability of stay of server under the influence of information security methods when attack is active, $P_3(t)$ is a probability of stay of server under the influence of information security methods, $\lambda(t)$, $\mu(t)$ are the intensities of flows of protective actions and informational attacks, that are chosen by players of conflict.

Table 3. The security level of security system during using strategy of withdrawal of player of influence to erroneous informational resource with further involving it in informational conflict

λ_1	λ_2	μ_1	μ_2	T=0,6 sec	T=0,8 sec	T=1 sec
0,00	0,00	1,00	1,00	1,000	1,000	1,000
0,50	0,50	0,50	0,50	0,768	0,707	0,646
0,50	0,50	0,50	1,00	0,774	0,712	0,646
0,50	0,50	1,00	0,50	0,774	0,712	0,646
0,50	0,50	1,00	1,00	0,780	0,717	0,646
0,50	0,75	0,50	0,50	0,715	0,636	0,549
0,50	0,75	0,50	1,00	0,720	0,633	0,529
0,50	0,75	1,00	0,50	0,717	0,633	0,532
0,50	0,75	1,00	1,00	0,722	0,630	0,512
0,50	1,00	0,50	0,50	0,663	0,560	0,438
0,50	1,00	0,50	1,00	0,662	0,541	0,380
0,50	1,00	1,00	0,50	0,661	0,547	0,401
0,50	1,00	1,00	1,00	0,660	0,528	0,344
0,75	0,50	0,50	0,50	0,715	0,636	0,549
0,75	0,50	0,50	1,00	0,717	0,633	0,532
0,75	0,50	1,00	0,50	0,720	0,633	0,529
0,75	0,50	1,00	1,00	0,722	0,630	0,512
0,75	0,75	0,50	0,50	0,662	0,558	0,434
0,75	0,75	0,50	1,00	0,660	0,541	0,385
0,75	0,75	1,00	0,50	0,660	0,541	0,385
0,75	0,75	1,00	1,00	0,659	0,524	0,336
0,75	1,00	0,50	0,50	0,606	0,472	0,296
0,75	1,00	0,50	1,00	0,597	0,432	0,197
0,75	1,00	1,00	0,50	0,598	0,438	0,215
0,75	1,00	1,00	1,00	0,589	0,398	0,116
1,00	0,50	0,50	0,50	0,663	0,560	0,438
1,00	0,50	0,50	1,00	0,661	0,547	0,401
1,00	0,50	1,00	0,50	0,662	0,541	0,380
1,00	0,50	1,00	1,00	0,660	0,528	0,344
1,00	0,75	0,50	0,50	0,606	0,472	0,296
1,00	0,75	0,50	1,00	0,598	0,438	0,215
1,00	0,75	1,00	0,50	0,597	0,432	0,197
1,00	0,75	1,00	1,00	0,589	0,398	0,116
1,00	1,00	0,50	0,50	0,547	0,371	0,125
1,00	1,00	0,50	1,00	0,528	0,307	0
1,00	1,00	1,00	0,50	0,528	0,307	0
1,00	1,00	1,00	1,00	0,508	0,243	0

For this strategy in work [4, 9] was shown, that that in case of arbitrary security strategies and influence the expression of evaluation (1) acquires the view:

$$I^*(\lambda_0,\mu_0)_{UA} = 1-\lambda_0 T^2 + \frac{1}{20}\lambda_0(18\lambda_0+7\mu_0)T^4 - \\ -\frac{1}{84}\lambda_0\left(3\lambda_0(18\lambda_0+7\mu_0)+\frac{1}{4}\mu_0(77\lambda_0+53\mu_0)\right)T^6$$

On base of this expression and step of change of λ parameters (the intensity of protective actions per unit of time), μ (the intensity of influences per unit of time) and time t, and using software «Optima – 2014 v.1.0», we have received the following dependences of security level (table 4).

As it is seen from the table 4 and fig. 7, if the players have chosen the optimal strategies of security and influence correspondingly, the predicted level of informational resource security using the strategy of estimation of security level using a pattern of normal system behavior, will be equal to 0,6044 (for $T = 1\text{sec}$), i.e. $I(\lambda^{opt},\mu^{opt}) \approx 0.215$. For the rest of occurrences, when the players evade from optimal strategies, this value varies in range of specified limitations.

Table 4. The security level of security system during using strategy of estimation of security level using a pattern of normal system behavior

λ	μ	T=0,2 sec	T=0,4 sec	T=0,6 sec	T=0,8 sec	T=1 sec
0,00	1,00	1,000	1,000	1,000	1,000	1,000
0,25	0,00	0,990	0,961	0,917	0,860	0,796
0,25	0,25	0,990	0,962	0,919	0,867	0,808
0,25	0,50	0,990	0,962	0,921	0,872	0,815
0,25	0,75	0,990	0,963	0,923	0,876	0,817
0,25	1,00	0,990	0,963	0,925	0,878	0,814
0,50	0,00	0,980	0,925	0,845	0,751	0,645
0,50	0,25	0,980	0,926	0,849	0,760	0,654
0,50	0,50	0,980	0,927	0,853	0,766	0,653
0,50	0,75	0,981	0,928	0,856	0,770	0,642
0,50	1,00	0,981	0,929	0,859	0,771	0,621
0,75	0,00	0,971	0,892	0,783	0,656	0,485
0,75	0,25	0,971	0,893	0,788	0,664	0,476
0,75	0,50	0,971	0,895	0,792	0,667	0,452
0,75	0,75	0,971	0,896	0,796	0,666	0,413
0,75	1,00	0,971	0,897	0,799	0,662	0,360
1,00	0,00	0,961	0,860	0,727	0,560	0,257
1,00	0,25	0,962	0,862	0,732	0,562	0,215
1,00	0,50	0,962	0,864	0,736	0,559	0,153
1,00	0,75	0,962	0,865	0,740	0,550	0,072
1,00	1,00	0,962	0,867	0,742	0,537	0

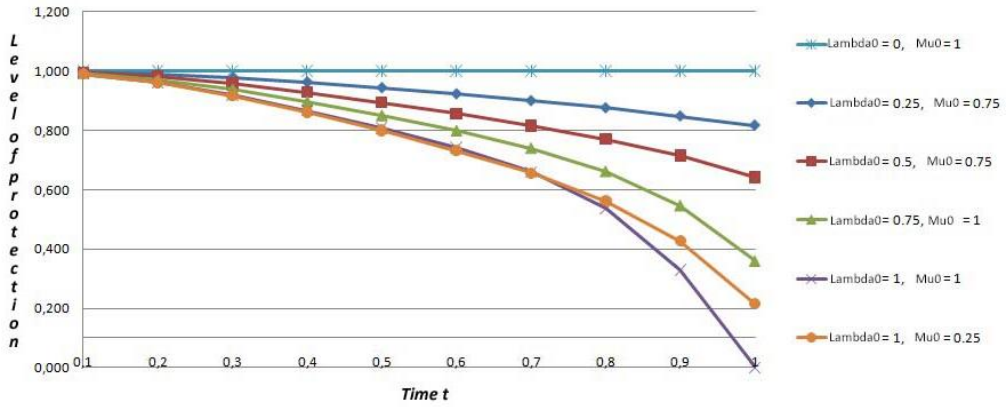

Fig.6. The dependence of security level $I(\lambda,\mu)$ on time t in case of using the strategy of estimation of security level using a pattern of normal system behavior

Therefore, with help of software «Optima – 2014 v.1.0», has been evaluated the predicted and current level of informational resources security for three strategies of forming the security systems: the strategy of forming of echelon security system, the strategy of withdrawal of player of influence to erroneous informational resource with further involving it in informational conflict and the strategy of estimation of security level using a pattern of

normal system behavior. In this work has been defined the predicted level of security of informational resource for each of examined strategies of forming the security system. As it is seen from results, the player of security can predict the security level and can optimize its resources, including those cases, when the player of influence uses optimal strategy.

In fig. 6 is shown the dependence of security level $I(\lambda,\mu)$ on time t.

B. Simulation of current is states for checking a possibility of identification a vulnerability of informational systems in under the conditions of influences

For evaluating the vulnerabilities of IS the following parameters have been chosen: the intensity of actions ($I_{actions}$), the capacity of used RAM (V_{RAM}), CPU load (P_{CPU}), the time of process preforming (T_{proc}), the quantity of executable processes (K_{ExProc}), the type of executable files of influence (F_{type}), the quantity of failures and errors ($K_{faliures}$), unusual processes ($K_{UnsualProc}$).

In process of attack (influence), the violator, influences on the system, changes its certain parameters, creates or stops processes that are peculiar to it etc. All these actions are reflected on the state of the system. Evaluating these parameters is possible to reveal the fact of influence and to identify the vulnerability of IS under conditions of influences [4,9]. So far the process of revelation and identification of vulnerability happens in case of uncertainty, and above mentioned parameters have not clear character, then the functioning of this system has to be based on non-precise logic. For identification the violator is possible to use logic-linguistic approach and base model of parameters, partly described in [2, 10, 12], which have been the base of developed software.

With help of developed software, using experimental approach has been developed a model of standards of linguistic variables for non-precise parameters of violator identification among chosen plurality of parameters using a work [5, 13, 16, 18].

Using an experimental approach, the rules have been formed, that they are aimed at vulnerabilities identification under conditions of influences. These rules allow to reveal anomalous state of IS, caused by violator activity, on base of using the methods of non-precise logic, expert estimations and models of standards of parameters, that are necessary for revealing the violator. Forming the rules has been carried out with help of corresponding model [3,13], and for creating it, the plurality of linguistic identifications has been brought in $LI = \bigcup_{i=1}^{d} LI = \{LI_1, LI_2, \ldots, LI_d\}$ where d is quantity of plurality elements, that are necessary for representation of anomalous state, and $LI_i \ (i = 1, d)$ elements of LI, each of them assumes one of the test values, that characterize in linguistic form the level of anomalous state of the system, that can be caused by attacking actions.

On base of plurality of identifications LI and set of linguistic links LC the plurality of rules has been formed for revealing vulnerabilities

$$ER = \left\{ \bigcup_{i=1}^{n} ER_i \right\} = \{ER_1, ER_2, \ldots, ER_n\}$$

where $ER_i \ (i = 1, n)$ – is a sub- plurality of possible rules for revealing i-th anomalous state, caused by i-th attack (influence), besides

$$\bigcup_{i=1}^{n} ER_i = \bigcup_{i=1}^{n} \left\{ \bigcup_{j=1}^{r_n} ER_{ij} \right\} = \{ER_{11}, ER_{12}, \ldots, ER_{1r_1}\},$$
$$\{ER_{21}, ER_{22}, \ldots, ER_{2r_2}\}, \ldots, \{ER_{n1}, ER_{n2}, \ldots, ER_{nr_n}\}$$

where $ER_{ij} \ (i = 1, n, j = 1, r_n)$ – is a j-th rule of i-th sub- plurality of possible rules, and a $r_i \ (i = 1, n)$ a general number of possible rules, intended for revealing of i-th anomaly. According to the work [3, 11, 15] is followed

$$ER = \bigcup_{i=1}^{n} \left\{ \bigcup_{j=1}^{r_i} ER_{ir_j} \right\} = \bigcup_{i=1}^{n} \left\{ \bigcup_{j=1}^{r_i} \left(LC_{ir_j} \rightarrow LI_{ir_j} \right) \right\} =$$
$$\left\{ \bigcup_{i=1}^{n} \left\{ \bigcup_{j=1}^{r_i} ER_{ir_j} = \left(LC_{ir_j} \rightarrow LI_{ir_j} \right) \right\} \right\}$$

where ER_{ir_j} is r_j-th rule of revealing anomaly, caused by *i*-th, that word for word is interpreted as: "If LC_{ir_j} is true, then the level of anomalous state, that can be caused by i-th attack, will be LI_{ir_j} ".

The developed software «Optima – 2014 v.1.0» allows to evaluate the predicted and current security level of informational resources for such strategies as the strategy of forming of echelon security system with *n* barriers of security; the strategy of withdrawal of player of influence to erroneous informational resource with further involving it in informational conflict; the strategy of estimation of security level using a pattern of normal system behavior. The received results have confirmed trustworthiness of developed method of optimization of information security systems behavior under conditions of influences.

V. Conclusions

Thus, in this article has been developed a method of optimization of information security systems behavior, that due to taking into account the parameters of security system (the quantity of security means, type of security sub-system, total security resource and value of

information), allows to define optimal behavior in system "influence-security". In addition, specialized software has been developed, that allows to verify the suggested method. The received results can be used for expansion of tools of groups of fast reaction to ISec incidents, ISec units of organization, and also for rising effectiveness of developing methods and information security systems.

ACKNOWLEDGEMENT

This scientific work was supported by RAMECS and CCNU16A02015.

REFERENCE

[1] A.A. Burushkin, A.A. Panfilov, Yu.K. Yazov, "Using the apparatus of Petri-Markov networks to assess the characteristics of the dynamics of the implementation of threats to information security in computer networks," *Counteraction to the Threats of Terrorism*: *ICSTT*, vol.10, pp. 162-169, 2007.

[2] Grischuk R.V. "The theoretical basis of modeling processes attacks on information theory methods of differential games and transformations: Monograph," *Exactly: Ruta*, 280 p., 2012.

[3] R.V. Grischuk, S.Z.H. Piskun, V.A. Khoroshko, J.E. Khokhlachova, "Gaming Methods of cyber attacks on information sphere" *Information Security*, vol. 1 no.54, pp. 86-93, 2012.

[4] Grischuk R.V., V.A. Khoroshko, "Synthesis of optimal behavior in the defense - attack system" *Problems creating, testing and maintenance of complex information systems*, vol. 5, pp. 60-66, 2011.

[5] Devyanyn V.D. "Models of computer security systems: Monograph", *Publishing Center "Academy"*, 144 p., 2005.

[6] V.E. Muhyn, A.N. Volokyta, "Complex Monitoring System based on security analysis purposes subject of computer systems and networks," *Control systems and machines*, vol.5, pp.85-92, 2006.

[7] Tereykovskyy I.A., "Neural networks in means of information security" *The Technical Writer's Handbook*, 209 p. 2007.

[8] Penrose R.A. "Generalized Inverse for Matrices", *Proceedings of the Cambridge Philosophical Society*", vol. 51, pp. 406-413, 1955.

[9] S.A. Gnatyuk, Y.E. Khokhlachova, A. Okhrimenko, A. Hrebenkova, "The theoretical basis of construction and operation of information security incident control," *Information Security*, vol. 1, no.54, – pp. 121-126, 2012.

[10] Khokhlachova Y.E., "Modeling optimality criteria and restrictions for the security of information systems" *Information Security*, vol.4, no.57, pp. 106-109, 2012.

[11] Y.E. Khokhlachova, S.S. Chumachenko, A.P. Duksenko, "Modern approaches to vulnerability assessment and modeling of information systems," *Journal of Engineering Academy of Ukraine*, vol. 4, pp. 121-126, 2014.

[12] V.A. Khoroshko, Y.E. Khokhlachova, "Assessment of security of information systems," *Current security* , vol. 4, pp. 50-58, 2012

[13] Y.E. Khokhlachova, "Information Security Policy Object," *Legal, regulatory and metrological support of information security in Ukraine*, vol.2, no.24, pp. 23-29, 2012.

[14] V.A. Khoroshko, I.S. Ivanchenko, Y.E. Khokhlachova "Evaluation of security communication systems in information and communications systems," *Information processing systems*, vol.3, no.110, pp.112-117, 2013.

[15] Opirskyy I.R., "Project design conflict threats complex system of information security in information networks of state," *Scientific Journal NLTU Ukraine, a collection of scientific works*, Issue 25.09, pp. 322-328, 2015.

[16] Opirskyy I.R. "Analysis of static models of unauthorized access to information networks State," *Międzynarodowy Zbiór prac naukowych «Współpraca Europejska»*, vol.2, no.9, pp-92-107, 2016.

[17] Zhengbing Hu, Vadym Mukhin, Yaroslav Kornaga, Yaroslav Lavrenko, Oleg Barabash, Oksana Herasymenko, "Analytical Assessment of Security Level of Distributed and Scalable Computer Systems", *International Journal of Intelligent Systems and Applications (IJISA)*, Vol.8, No.12, pp.57-64, 2016. DOI: 10.5815/ijisa.2016.12.07

[18] Dudykevych V.B., Opirskyy I.R., "Analysis models of information security in information networks of state". *Information processing systems*, Issue 4 no.141, pp. 86-90, 2016.

[19] Sudhir Kumar Sharma, Ximi Hoque,"Sentiment Predictions using Support Vector Machines for Odd-Even Formula in Delhi", *International Journal of Intelligent Systems and Applications(IJISA)*, Vol.9, No.7, pp.61-69, 2017. DOI: 10.5815/ijisa.2017.07.07

[20] Zhenbing Hu, Vadym Mukhin, Yaroslav Kornaga, Yaroslav Lavrenko, Oksana Herasymenko,"Distributed Computer System Resources Control Mechanism Based on Network-Centric Approach", International Journal of Intelligent Systems and Applications(IJISA), Vol.9, No.7, pp.41-51, 2017. DOI: 10.5815/ijisa.2017.07.05.

Authors' Profiles

Zhengbing Hu

PhD, Associate Professor of School of Educational Information Technology, Central China Normal University, M.Sc. (2002), Ph.D. (2006) from the National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute". Postdoc (2008), Huazhong University of Science and Technology, China. Honorary Associate Researcher (2012), Hong Kong University, Hong Kong. Major research interests: Computer Science and Technology Applications, Artificial Intelligence, Network Security, Communications, Data Processing, Cloud Computing, Education Technology.

Yulia Ye. Khokhlachova has received PhD in Eng degree at National Aviation University (Information Security) in 2015. From 2016 she is Associate Professor at Academic Dept of ITSecurity in National Aviation University (Kyiv, Ukraine). Research interests: network & internet security, cybersecurity.

Viktoriia Sydorenko: PhD Student (2012-2015), Assistant Teacher (from 2013). In 2012 she received MSc degree in Information Security from NAU. She is currently working at NAU in Academic Department of IT-Security. Research interests: Computer Network & Internet Security, Cybersecurity & Critical Information Infrastructure Protection.

Ivan R. Opirskyy was born in 1987 in Simferopol, Crimea, Ukraine. In 2008 he graduated from the National University "Lviv Polytechnic" and received a Master degree in "security of information with restricted access and automation of its quitrents." In 2012 he received his PhD. on specialty "Information security systems" at the National University "Lviv Polytechnic". Since 2016 is assistant professor of information security departmentat the National University “Lviv Polytechnic”. Research interests: information security systems, physical security of objects, forecasting unauthorized access, communication channels security, cybersecurity, integrated security systems, ensuring information security.

How to cite this paper: Zhengbing Hu, Yulia Khokhlachova, Viktoriia Sydorenko, Ivan Opirskyy, "Method for Optimization of Information Security Systems Behavior under Conditions of Influences", International Journal of Intelligent Systems and Applications(IJISA), Vol.9, No.12, pp.46-58, 2017. DOI: 10.5815/ijisa.2017.12.05

