Simulation and evaluation of conflict interactions in information systems

N I Goncharov, A V Dushkin, I V Goncharov and P A Parinov
ET Department, Voronezh Institute Federal Penitentiary Service of Russia, 1a Irkutskaya Street, Voronezh, RU

E-mail: a_dushkin@mail.ru

Abstract. The work describes the scenario of conflict interactions in information system and intruder security using the formalism of hybrid automata. Analysis of probability of winning on both sides in the conflict. The possibility of abstraction from a concrete kind of density distributions for the time the parties to the conflict in their possible States. Based on the destructive effects of information distribution models in information system shows the mutual influence of the spread of the destructive processes information on process state changes subjects information system. With this approach, based on a view of information system in the form of a two-dimensional cellular automaton. The results of experimental research of confirming the theoretical conclusions.

1. Introduction
In the study of the security of information systems, built using modern technology, it is important to consider two main clusters: directly related to the possibility of a security breach information information system; associated with the possible spread of destructive information impacts in information systems. In practice, the processes associated with both groups listed the issues are inextricably linked and require integrated treatment, taking into account the particularities of the provisions conflict theory in modeling processes in different information systems [1-5]. This can be ensured by using the proposed next models: conflict interaction of information systems and intruder security information based on the formalism of hybrid automata; the proliferation of destructive information impacts in information systems entities taking into account internal factors of the system and their status based on the model of cellular automata.

2. Modeling of processes of conflict information system and information security violator
The first challenge is the rationale for the model of conflict interaction of information systems and information security violator. In the framework of the proposed next model built using the formalism of hybrid automata is solved the problem of ratios to assess the probability and estimated lower bound estimates of the probability of a security breach information information system on the basis of the most common options, such as the mathematical expectation and variance for time information system and the violator in each of its discrete States. Basic properties of hybrid automata and their application to problems of modeling conflict interactions systems discussed in previous works of the authors [6-8].
Let one of the parties to the conflict (side a) is the information system. A positive result of the work of the information systems security is circulating the information within a specified interval of time \(0 \leq t \leq T\). While information systems all the time is in a group of conditions specific to its operation and functioning in regular mode. Loss of information systems in conflict is violation of the information circulating in security, accompanied by the corresponding transition in critical condition. The second party to the conflict (side B) is a system that wrongdoing has the purpose to disturb the security of the information circulating in a, which means the translation of information systems in critical condition within a specified interval of time. Achieving this result determines the payout system. Lost in here arises in the case of not achieving a result for the allotted period of time \(0 \leq t \leq T\).

In shown in figure 1 has two parallel models of hybrid automata: mechanical and automatic. For these machines many discrete variables \(S^D = \{s_a, s_b\}\), describe the basic condition, represented by two variables, each of which accepts values \(s_a \in Q_A = \{L_A, D_A\}\). \(s_b \in Q_B = \{L_B, D_B\}\). Condition \(L_A\) Here denotes the operation until the use of enemy vulnerabilities available, leading to a breach of information security in information systems and the transition to a critical state \(D_A\) («lost» \(A\)). Condition \(L_B\) denotes the operation of \(B\) with a view to disrupting \(A\), until the expiry of the time allotted, that leads to bad the attacker to compromise the information within a period of time («lost» \(B\)) and the corresponding transition in Condition \(D_B\). Transition in \(D_A\) and \(D_B\) going in leaps and bounds under the influence of events \(\text{attack}_B\) \(t \geq T\), define, respectively, lost to \(A\) and \(B\).

For a detailed description of the conduct of the parties in conflict internal condition of many as nested hybrid machines that will call the hybrid machines active items.

A subset of characters \(Q^L_{A0} = \{A_0\}\) consists of the symbol of one State, which stands for preparatory actions for the Organization and bring the system to A working state. A subset of characters \(Q^L_{A1} = \{A_1, A_2\}\) indicates the status of the active work of the system in normal mode and are nested to general condition that is treated as «A system protected against all known vulnerabilities». A subset of characters \(Q^L_{A2} = \{A_2\}\) indicates the status of the system in the face of (open) new vulnerability. They are nested to general condition \(A_2\), which is treated as «A system is not protected from the vulnerability open». The transition from a State of \(A_i\) in condition \(A_i\) is under the influence of events vulnerability with the condition that this vulnerability opens on time interval \([t, T]\), designated conflict interaction systems. To describe the process of vulnerabilities used external model random events. The transition from a State of \(A_2\) back to \(A_1\) is subject to successful completion of the works to close vulnerabilities in \(A_2\). For the active elements of the parties when implementation of the simulation within a typed description of conflict prompted the following States and transitions. A subset of characters \(Q^L_{B0} = \{B_0\}\) consists of the symbol of one State, which stands for preparatory actions for the Organization and bring the system to the operating state («deployment» \(B\)) that are executed once without returning and repetition. A subset of characters \(Q^L_{B1} = \{B_1, B_2\}\) refers to a group of States of the system \(B\) mode the search and discovery of vulnerabilities when finding A system able to \(A_i\) (A protected against all known vulnerabilities).
Condition $B_{11}$ here defines the operation of the system, which includes the collection of data on A system (analysis of organizational design principles used technical equipment and software, and the qualifications of users and rights the staff). Condition $B_{12}$ defines actions aimed at finding vulnerabilities at work (A) in normal mode. Probability $P_{B_{12}}$ set within the local operator of conduct as the probability of a successful vulnerability detection with A functioning normally and does not depend on time. In the model presented in figure 1., in addition to the main, displayed another passage from $B_{12}$ in the next group of discrete States. It is attributable to the events of the vulnerability (opening new vulnerability) that occurs in the interval $[t, T)$. When it is accepted that the information about the opening of new vulnerabilities (A) and (B) is obtained from external Wednesday simultaneously. A subset of characters $Q^L_{B_{12}} = \{B_{21}, B_{22}\}$ indicates the status of the system (B) after receiving information about a detected vulnerability. Here the State of $B_{21}$ defines actions aimed at vulnerability analysis for its use and has a finite time. Status $B_{22}$ defines the holding action to use the vulnerability to compromise the security of information systems (A). A subset of characters $Q^L_{B_{12}} = \{B_{v}\}$ consists of the symbol of a one condition called State of successful information security breaches in information systems. Transition in critical condition is accompanied by the creation of events attack_A the transferor of the hybrid machines A from condition of $L_A$ in its own condition $D_A$. Condition $B_v$ in

![Figure 1. View conflict information system interoperability and information security intruder using hybrid automata.](image-url)
this model, is absorbing. The transition from a condition of $B_{22}$ in its own condition $B_{12}$ is carried out in a failed attempt to use the previously discovered vulnerabilities.

2.1. The assessment of the potential security breach information

Next, for example, are received by the authors of analytical equations for analysis of the probability of winning a hand $B$ [6-8] without external information about a new vulnerability. An analytical ratio based on Gaussian approximation for random variable $\tau_{b,1}$:

$$P_{\tau_{B,1}}^{(i)} = \Pr(0 < \tau_{B,1} < T) = \int_0^T N(u, m_{B,1}, d_{B,1}) du =$$

$$= F\left(\frac{T - m_{B,1}}{\sqrt{d_{B,1}}}\right) - F\left(\frac{-m_{B,1}}{\sqrt{d_{B,1}}}\right),$$

(1)

$$F(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^x N(v, 0, 1) dv,$$

where $N(u, m, d)$ — designation Gaussian density probability distribution with the appropriate parameters. To assess likelihood lower bound violations of information security can use Chebyshev inequality [6-8] as well, you can refine this assessment on the basis of inequality Vysochansky-Petunina, assuming that the density distribution composition $\tau_{b,1}$ is a unimodel:

$$P_{\tau_{B,1}} = \Pr[\tau_{B,1} \leq T] \geq \Pr[|\tau_{B,1} - m_{B,1}| < T - m_{B,1}] =$$

$$= \Pr\left[|\tau_{B,1} - m_{B,1}| < \frac{T - m_{B,1}}{\sqrt{d_{B,1}}}\sqrt{d_{B,1}}\right] \geq$$

$$\geq 1 - \frac{4}{9\rho^2} = 1 - \frac{4d_{B,1}}{9(T - m_{B,1})^2},$$

(2)

$$\rho = \frac{T - m_{B,1}}{\sqrt{d_{B,1}}} \geq \frac{8}{3}.$$ 

Much more difficult is the task of assessing the likelihood of winning (B) provided that the analyzed time interval received information on the opening of this new vulnerability. Analytical ratios for this assessment also received the authors in the light of the introduction of certain assumptions and approximations, but their description is beyond the scope of this publication.

2.2. The results of the experiment

Checking possibilities of analytical ratios carried out using different types of distributions for the time of stay of systems in their States. For many statistical experiments, each of which consisted of 1000 trials, dealt with various combinations of distribution laws, their parameters and return probabilities for a repeat performance. The results reduced the probability of winning to dependencies $P$ from $\rho = (T - m_{B,1})^2 / d_{B,1}$. A few examples of such the dependencies shown in Figure 2.

In Figure 2 it is shown, that application of analytical ratios based on inequalities Vysochansky and approximation of Gauss Petunina-allows to obtain reasonably accurate lower bounds of probability and realistic estimate the probability of a security breach information Accordingly, in uncertainty distribution densities for time information system and intruder security information in their condition. More than rough estimates allows you to receive an analytical ratio, obtained on the basis of Chebyshev's inequality. In this case, the accuracy of analytical relations is determined by the
parameters defined in each case and input assumptions. Without the introduction of specific assumptions, paid when calculating using the analytical error ratios, leveled possible errors in choosing distribution laws, if you set them explicitly.

Figure 2. The results compare with the results of the evaluations received simulation.

Of the dependencies shown in figure 2 designed for specific information systems, the overall conclusion that the higher the value of the parameter \( \rho \), characterizing the relative difference between the total average time review of the conflict and the time necessary to compromise the security of information, the greater the likelihood of violations of information security in the information system. This underlines the importance of the time factor when implementing proactive intervention versus the probability of «losing» in the final stages of the vulnerabilities in the information system and their use.

3. Modeling the spread of destructive information in information system

Modeling and analysis of the spread of destructive information influences are encouraged to use an approach based on a view of information systems as a two-dimensional cellular automaton. Two-dimensional cellular automata can be defined as the set of finite state machines (information systems entities), placed on a plane and tagged integer coordinates \((i, j)\), each of which can have certain properties, and is located in one of the condition \( S_{i,j} \in \{S_1,S_2,...,S_k\} \). State of the state machine \((i, j)\) at the time of the \( t + 1 \) s defined as follows:

\[
S_{i,j}(t + 1) = F(S_{i,j}(t), N(i, j), t),
\]  

where \( F \) – the rule change States in the automaton; \( N(i, j) \) – the neighborhood of a point \((i, j)\); \( t \) – step on the time axis.

Cellular automaton model every cell changes its State in the course of interaction with a limited number of cells, usually with those with whom it has shared the side or the top. This enables you to bind the processes occurring at the micro level, the processes of spatial interaction between the elements.

To describe the process of dissemination of destructive information in information systems, we propose the following model. Communication information systems is represented as a two-dimensional cellular automaton, lattice which implements a two-dimensional array, and each cell is numbered ordered pairs of numbers \((i, j)\). Each cell is the subject of information systems. The immediate neighbours of each cell are considered cells with the original common vertex (Moore neighborhood), such cells would be 8.
To eliminate edge effects grid cellular automaton topologically «collapse into Tor» [9], i.e., the first line is considered a continuation of the last, and the last is previous first. Similarly come with columns [9]. Each cell can be in one of the States: S0 is the initial state; S1 is the State in which the subject has developed resistance destructive information impacts, but does not distribute it; S2 is the State in which the entity has adopted a destructive information impacts, but does not distribute it; S3 is the State in which the subject has developed and disseminated opposition to destructive informational influences; S4-a condition in which the subject adopted destructive impacts information and circulates it. Depending on the condition and internal features, a cell can spread destructive informational influences (affect neighboring cells), and do not distribute. Changing conditions and behavior of the cells is carried out on the basis of the proposed model rules. These rules take into account internal factors of the subjects of the information systems and their status. The navigation scheme of the subject from State to State is represented in figure 3.

The actor, who provided information about the destructive impacts of information systems, can take this influence or resist it. Depending on the internal factors of the subject, it can continue to disseminate information about the destructive impacts of information systems, and distribute.

**Figure 3.** Graph navigation scheme of the condition into condition.

Simulation algorithm is as follows: during the preparatory stage identifies the main characteristics of the subjects of the information systems; in the first phase of the simulation, the corresponding zero step on time \( t = 0 \), all field consists of cells able to \( S_0 \), with the exception of a few cells, which are pioneering the spread of destructive informational influences; the second stage is the proliferation of destructive information influences in step time \( t = t + 1 \), internal parameters are calculated on the basis of the proposed subjects above models, cells whose value transfer of destructive information impacts equal to 1, transmit information to neighbouring cells.

### 3.1. An example of the results

In figure 4 the work machine for the case where most of the actors have a neutral attitude to destructive information influences. In figure 5 the work machine for the case where most of the actors have a negative attitude towards destructive information influences. In figure 6 Delt machine when most subjects have a positive attitude towards destructive information influences. The figures «a» the work machine for the case where actors take destructive information influences interacting with them actors. figures «b» Delt machine for the case when the subject could generate opposition to destructive information influences.

Analysis of the figures shows that the 4-6:

- the spread of destructive information influences the nature of information systems, close to exponential;
- in the case of neutrality (fig. 4A) to the destructive information impacts, a small number of initiators is enough for successful implementation of destructive informational influences;
- in the case of a deliberately negative or positive attitude (fig. 5A and 6A) actors to destructive information impacts their status during the destructive impacts of information does not change;
- in the case where the actors can develop resistance to destructive informational influences (fig. 4B, 5B, and 6B), the number of subjects in S3 and S4 is the same, regardless of their initial state.

The application of the proposed model allows you to associate the spread of destructive information in information systems and process state changes when communicating information systems entities related subjects.

**Figure 4.** Distribution of cells depending on the discrete time (most of the actors have a neutral attitude to the destructive effects of information).

**Figure 5.** Distribution of cells depending on the discrete time (most of the actors have a negative attitude towards the destructive impacts of information).
Figure 6. Distribution of cells depending on the discrete time (most of the actors have a positive attitude towards the destructive impacts of information).

4. Conclusion
The authors model of conflict interaction of information systems and information security and the infringer received as part of her analytical equations for probability assessment and evaluation estimated lower bound the probability of infringement information system security, allow you to abstract from the specific type of density distributions for the time of stay of parties in their possible States. Application of this model is relevant for the decision of tasks of study information systems security for various purposes. The proposed model the spread of destructive information in information systems allows you to link the spread of destructive information in information systems and process state changes subjects information systems under the influence of related subjects that is relevant in considering the issues of security of information systems, built using modern information

References
[1] Dushkin A V, Kochedykov S S, Noev A N and Gubin I A 2018 Method of optimum channel switching in equipment of infocommunication network in conditions of cyber attacks to their telecommunication infrastructure International Conference Information Technologies in Business and Industry IOP Conf. Series: Journal of Physics: 1015 032101. DOI:10.1088/1742-6596/1015/3/032101 pp 187-193
[2] Dushkin A V, Kochedykov S S and Novoseltsev V I 2017 Tool and algorithmic diagnostic devices of operability of actuation mechanisms of automated control systems Proceedings. 2017 2nd International Ural Conference on Measurements (UralCon) South Ural State University (national research university), Chelyabinsk, Russian Federation DOI: 10.1109 URALCON 8120709 pp 193-198
[3] Balan V P, Novoseltsev V I, Dushkin A V and Sumin V I 2015 Conflictology: tutorial (M: Hot line-Telecom) p 342
[4] Balan V P, Novoseltsev V I, Dushkin A V and Sumin V I 2015 Conflict management (M.: Hotline-Telecom) p 144.
[5] Dushkin A V, Kochedykov S S, Novoseltsev V I, V I Sumin and Eliseyev A I 2017 Mathematical model of information processing and protection in automated systems manage critical objects, taking into account the mutual influence of software components in exposure to information security threats Industrial Automated Control Systems and controllers 9 pp 33-46
[6] Dushkin A V, Kochedykov S S, Sokolov V I and Novoseltsev V I 2017 Simulation system of conflict interactions in information system critical applications Herald of the Voronezh Institute of the Federal Penal Correction Service 4 pp 74-84
[7] Dushkin A V, Kochedykov S S, Novoseltsev V I, Zdolnik V V and Minin Yu V 2018 Mathematical models of cyber threats to the software of the automated control system. *Industrial Automated Control Systems and controllers* 2 pp 43-55

[8] Barkalov S A, Dushkin A V, Kolodyazhny S A and Sumin V I 2017 Introduction to system analysis (Moscow: Hot line-Telecom) p 234

[9] Dushkin A V, Novoseltsev V I and Sumin V I 2015 *Simulation management systems and information technology support: tutorial* (M: Hot line-Telecom) p 192

[10] Kochedykov S S, Dushkin A V, Novoseltsev V I and Sumin V I 2016 Optimization of information flow in systems critical assignment in terms of third-party forces *Gazette of the Voronezh Institute of the Federal Penal Correction Service* 4 pp 67-72

[11] Dushkin A V, Pohvashhev V N and Sokolovsky S P 2011 Way malware recognition impacts on information system *Telecommunications* 10 pp 25-28

[12] Dushkin A V and Sokolovsky S P 2010 Neural network implementation of the module detecting Unauthorized Access at Itks *Information and security* 1 pp 123-126

[13] Dushkin A V and Scherbakov Yu V 2014 Safety assessment processes information in applying promising cloud technologies in MIS *Gazette of the Voronezh Institute of the Federal Penal Correction Service* 1 pp 21-25

[14] Dushkin A, Goncharov I, Goncharov N, Parinov P and Kochedykov S 2018 *Probabilistic Analysis of the Influence of Staff Qualification and Information-Psychological Conditions on the Level of Systems Information Security* Probabilistic Modeling in System Engineering UK (London: IntechOpen) DOI: 10.5772 pp 233-253

[15] Goncharov I V and Sirota A A 2018 Modeling conflict interaction systems using the formalism of hybrid automata *Information technology* 1 pp 17-27

[16] Goncharov N I and A A 2017 Sirota Study conflict coalitions systems using the formalism of hybrid automata *System analysis and information technologies* 4 pp 56-70

[17] Goncharov I V and P A Parinov A A 2018 Sirota modeling of processes of the information-psychological influence in social networks *System analysis and information technologies* 2 pp 93-104