UDC 004.056.5

DEVELOPMENT OF AN ALGORITHMIC SYSTEM FOR DETECTING AND DISARMING THREATS BASED ON FUNCTIONING TABLES

[1] I.Kh. Normatov, [2] M. Atazhanov, [3] R. Karimov
[1,3]*National University of Uzbekistan named after Mirzo Ulugbek, Tashkent, Uzbekistan*
[2]*Military Academic Lyceum named after Jaloladdin Manguberdi, Urgench, Khorezm*

Abstract. The article provides an analysis of known existing systems designed to collect and automatically analyze events of various information in order to identify threats. Their disadvantages are given. An algorithmic model of information security based on tables of functioning is proposed as a mathematical tool for modeling dynamic discrete systems for detecting and neutralizing threats while ensuring information protection. A method for assessing information security risks and ensuring the confidentiality of information resources is given. The features of working with data flows, management and control over them are considered. mathematical solutions for assessing the protection of information resources and various aspects of assessing the economic effectiveness of ensuring the confidentiality of information resources are presented. One of the ways of analyzing the security of the system is proposed - the construction of dynamic tables of functioning. The description of the main functions and requirements of automatic threat detection and neutralization based on the tables of operation based on the functioning tables (FT) is considered.

Keywords: algorithm; mathematical: information and algorithmic models; information system; functioning table: threats: risks; detection: neutralization.

Introduction

The evolution of information technologies is associated with intelligent systems, which include processes of origin, adaptation and development. It is the systemic approach to IT that determines the methods and algorithms for building systems. The systemic approach to information security (IS) requires identifying its subjects, means and objects, principles of provision, sources of danger, and the direction of dangerous information flows.

The modeling principle allows avoiding errors in designing effective systems. When developing an effective system, the principle of communication comprehensively considers the object of protection, combining the external environment, means of protection and aggressive threats and taking into account the interrelations: source of threat – weakness – action – attack.

The development of a security system is the main condition for ensuring the security of confidential information in an information system, is formulated by studying the system requirements for the system and is aimed at neutralizing system vulnerabilities.

One of the methods of system security analysis is based on dynamic FT of the information system based on Petri nets [3-6]. Based on FT, the operability of the implemented security system is checked and its shortcomings are identified, i.e. with the help of **FT**, it is determined what actions occur in the system, what states were before these actions and what states the system takes after the action is completed.

Thus, the performance table calculates all risks that threaten the system and valuable information in the system.

Main part

One of the main methods of analyzing the security of systems is the construction of dynamic tables of the IS [1–6]. Algorithmic models based on FT [1, 2] represent a mathematical apparatus for protecting information systems from external and internal threats and are divided into several types:

– a general structural model of ensuring information system security based on FT;

– a mathematical model for identifying threats from external and internal sources;

– synthesis and analysis of the construction of the FT after receiving the necessary data at the "synthesis" stage;

– ways, methods, models and means of destroying detected threats;

– analysis of the information system and threats in the system.

Development of FT and flow chart of threats. The most convenient way to visually display actions in the system is to use a Petri net. The principle of operation and the state of the networkit is determined by itmarked graph anddistribution of chips by positions. The vertices of the graph are the network markings, the arcs are defined by the transition symbol and are constructed for each active transition. Construction stops when there are no activated transitions on the graph or there are no markings. Let us assume that the graph of reachable markings is an automaton. For example, the trajectories in the Petri net are defined as follows (Fig. 1).

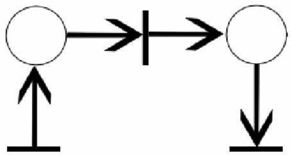

Fig. 1. Trajectory of Petri net movement

At each time interval $t_1 \in T$ the description of the FT is presented in the form of a labeled Petri net: $M = \{P, D, I, O, \mu\}$, where P – sets of positions (states), D – operations (transitions), I– input and O – output states, μ – a function that displays the set of positions in the set of natural numbers N those. $\mu : P \rightarrow N$. Each marking μ can be represented as a vector $\mu = (\mu_1, \mu_2, \ldots, \mu_n)$, where $n = |N|$ and $\forall \mu_i \in N$, $i = \overline{1,n}$. Vector μ defines for each position p_i, $i = \overline{1,n}$ network number of chips, i.e. $\mu(p_i) = \mu_i$, $i = \overline{1,n}$.

The designed FT visually displays all identified threats in the system we protect. After identification by the Petri net graph, all threats move vertically downwards only if it is a threat of the same type. In the example of the following type. The Petri graph goes through such an action due to the uniformity of the threat. Because each O_i – this is one of the types of threats in the GOST "Information technologies, information security, terms and definitions". All of the information security management threats, risks, attacks, methods and means of information protection, protection of sensitive information, information security of telecommunications and mobile networks, data protection and recovery, copy protection and others listed in this information security management standard are distributed in the FT according to their characteristics and the logical actions they perform (Fig. 2).

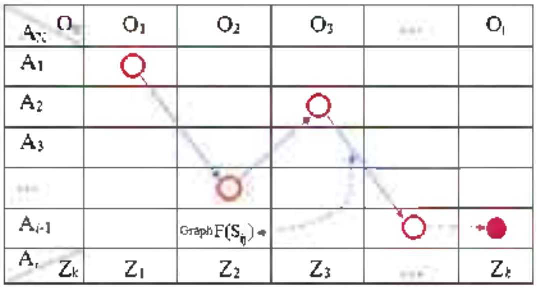

Fig. 2. Functioning table

If the machines are unable to process and destroy threats, then the task is passed on to another machine below. If the threat is combined, then the graph's actions take on a completely different form.

Let's consider the first case, that is, the threat *AB*, which comes from the Internet and consists of two separate parts *A* and *B* (where *A* – utility, driver, image, simple file, etc., *B* – background threat hidden in *A*). In this case, the threat will be pre-processed, blocked and removed before it can cause damage to the system. *A* after the user takes the link to *AB* on the Internet and launch *AB* in the FT network the link will be divided into two parts: *A* and *B* (Fig. 3).

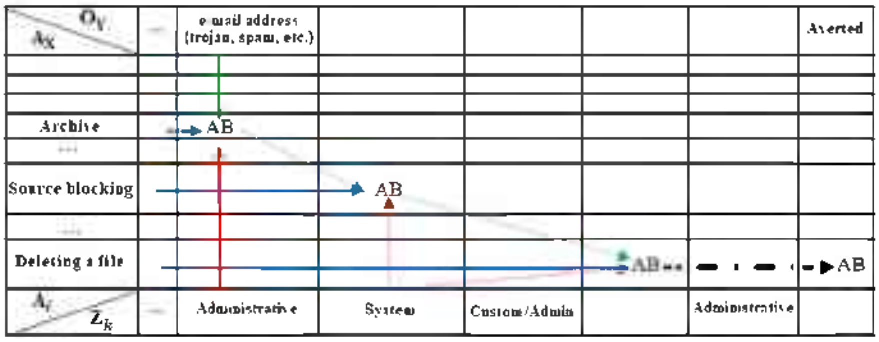

Fig. 3. The first case of the functioning table

In the second case, the threat is considered for the first time, and each of its passages is designated separately. O_Y the row of tables of cases 1 and 2 contains potential threats to the system. In table of cases 2, the paths of threats are shown in red, the prevention of threats is shown in green, and the transition of existing threats to another cell and their prevention is shown in black (Fig. 4).

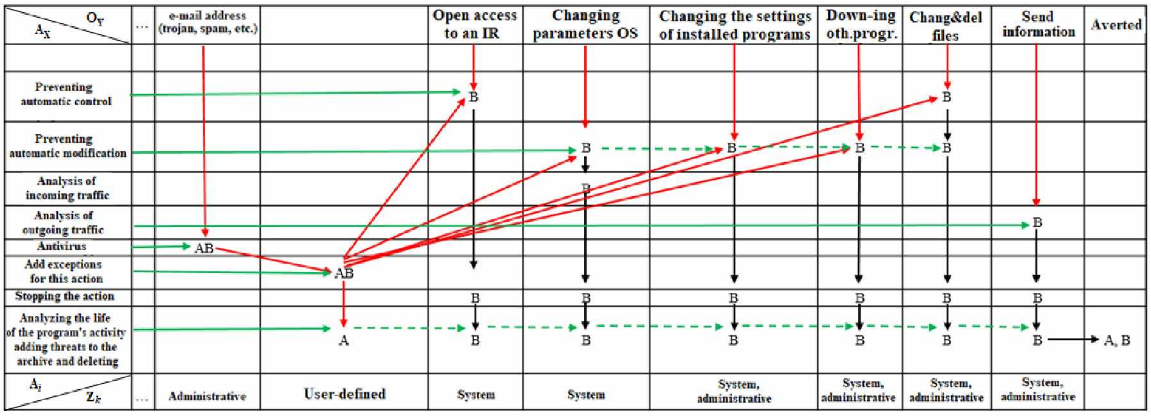
O_Y
A_X
...
e-mail address (trojan, spam, etc.)
Open access to an IR
Changing parameters OS
Changing the settings of installed programs
Down-ing oth.progr.
Chang&del files
Send information
Averted
Preventing automatic control
Preventing automatic modification
Analysis of incoming traffic
Analysis of outgoing traffic
Antivirus
Add exceptions for this action
Stopping the action
Analyzing the life of the program's activity adding threats to the archive and deleting
AB
AB
A
B
A, B
A_j
Z_k
...
Administrative
User-defined
System
System
System, administrative
System, administrative
System, administrative
System, administrative

Fig. 4. The second case of the functioning table

The second part can run malicious parts of its program and download other malicious programs without the administrator's permission.

The transition process is calculated as follows. There are 127 threat defenses in the table vertically. If the penetrating threat is a combined one, then it is checked in each cell. To calculate a more effective transition to destroy threats, we have the formula: $P=\sum_{i=1}^{\infty} U_i$, where U – threat, P – transitions by FT. Let A – means of protection against threats, K – class of threats. Then $U=1$, $P_{\max}=127$ and when $U=2$, $P_{\max}=254$. So $P_{\max}=U*A$.

If the class of threats is defined and the ways of destroying the threat are also clear according to the class, then the formula will be as follows: $P_{\max i}=U(A-(A-K_i))$, $i=\overline{1,9}$. If one of the classes of threats is not defined, then it is equal to zero.

Since threats penetrate in a variety of ways, it is impossible to use one or several of them to calculate an effective way to eliminate threats. It is necessary to use all means of protection against threats. So, transitions along the FT are equal to $P=\sum_{i=1}^{9} P_{\max i}$.

If the penetrating threat is not combined then the maximum processing cell will be calculated vertically by reading the lines, and the minimum will be equal to one.

Conclusion

Thus, in the work, various information events collected for the purpose of identifying threats and their automatic analysis allow developing an effective program for identifying and neutralizing threats to information security. The proposed algorithmic model of information security based on the tables of functioning serves as a mathematical apparatus for modeling dynamic discrete systems for identifying and neutralizing threats when ensuring information security. After the software is launched, threats are launched simultaneously with it, as a result of which the proposed system begins to combat these threats. In most cases, this conflict has the form of an asterisk, and the reason for its distribution in this form is that the conditions for the penetration of a threat in the form of a set are accepted here. The tables of functioning represent an algorithmic model of an automated control system for ensuring the security of information systems, as well as preventing any threats to information systems and information resources.

References

1. Glushkov V.M. Introduction to ACS. Kyiv: Tekhnika, 1972.

2. Zhuravlev Yu.I. Discrete Mathematics and Mathematical Questions of Cybernetics. M.: Nauka, 1974.

3. Peterson J. Petri net theory and systems modeling. Moscow: Mir, 1984.

4. Marchenkov A.E. Systems approach in research of management of innovative activity of integrated structures // Problems of Radio Electronics" EVT series, 2012. iss. 2. 189–196.

5. Normatov I.Kh., Toshmatov S., Yarashov I. Research and modeling of authentication process using functioning table // Journal of Mathematics, Mechanics and Computer Science, 124 (4), 71–85.

6. Normatov I. Endless individual areas of logic and beginnings of arithmetics // Modern problems of applied mathematics and information technology, 2023, 020008.

7. Normatov I., Yarashov I., Otakhonov A., Ergashev B. Construction of reliable well distribution functions based on the principle of invariance for convenient user access control // 2022 International Conference on Information Science and Communications Technologies, ICISCT 2022.

8. Normatov I.Kh., Ibadullaev D., Tangriberdiev O. Algorithm for constructing a non-degenerated quadratic stochastic operator by binomial distributions // Materials of 8th International conference "Actual problems of applied mathematics and information technologies", 2023, 133–135.

9. Normatov I., Yarashov I., Toshmatov S. Research and modeling of authentication process using functioning table // KazNU Bulletin. Mathematics, Mechanics, Computer Science Series. 2024, 124(4), 71–85.

Information about the authors

Normatov I.Kh., Doctor of Physical and Mathematical Sciences, Professor, Director of the Scientific and Innovation Center "Digital Technologies and Cybersecurity" named after Academician V.K. Kabulov at the National University of Uzbekistan named after Mirzo Ulugbek, i_normatov@nuu.uz.

Atazhonov M.N., Teacher of the Military Academic Lyceum named after Jalaluddin Manguberdi, muzaffar19910627@gmail.com.

Karimov R., Basic doctoral student of the National university of Uzbekistan named after Mirzo Ulugbek, karimov_r@nuu.uz.