TEKA. COMMISSION OF MOTORIZATION AND ENERGETICS IN AGRICULTURE – 2014, Vol. 14, No.1, 134-143

Information security of critical application data processing systems

Valerie Lahno

Department of Economic Cybernetics, Lugansk National Agrarian University,
Town LNAU, Lugansk, 91000, Ukraine, e-mail:ss21@meta.ua

Received January 20.2014: accepted February 13.2014

Summary. The results of researches, allowing to raise the level of protection of the automated data processing systems of critical applications (ADPS CA) and intellectual information systems of enterprises are presented in the article. The mathematical models and results of vulnerability estimation of information systems which have Internet connection through various communication channels are resulted in this work. The system approach to solving problems of information security, proposed in this work provides for the integration of mathematical models of the processing and protection of information. The method of modeling the security policy (SP) to provide a highly reliable information processing (HRIP) has been developed. The mathematical models of synthesis of policy safe interaction of information processes, allowing SP to consider separately the various structural components of network with the ability to its further interlinkages have been developed. Using the new mathematical models of flexible reliability, availability, confidentiality and integrity of information processed, allowing mathematically describe the mechanisms to ensure the availability and confidentiality of the information and take into account the quantitative requirements for data integrity.

Key words: Protection of Information, the data processing system, security policy, mathematical models.

INTRODUCTION

The modern approach to ensure the reliability of information processes (IP) and its protection from unauthorized access (UA) is supported at the international level by standard ISO/IEC 15408. According to this approach, a reliable IP successfully counteracts to the specified threats of security at the given external conditions of its operation. This leads to continuous improvement as ways and means of information protection (MIP) as well as ways and means of implementation of threats to information security (IS), resulting that appearance of new MIP leads to its bypassing by means of attack [1, 2, 4, 25].

This, in its turn leads to the need for a new interpretation of the term "reliability of IP" that should be understand as lack of security vulnerabilities, which can be a consequence of the implementation of the various unintentional and intentional threats [3, 9, 13, 27].

The sophistication and effectiveness of cyberattacks have steadily advanced. These attacks often take advantage of flaws in software code, use exploits that can circumvent signature-based tools that commonly identify and prevent known threats, and social engineering techniques designed to trick the unsuspecting user into divulging sensitive information or propagating attacks [16, 24, 30, 31]. These attacks are becoming increasingly automated with the use of botnets

- compromised computers that can be remotely controlled by attackers to automatically launch attacks. Bots (short for robots) have become a key automation tool to speed the infection of vulnerable systems [5, 11, 14, 23].

Analysis of existing methods of HRIP modeling that affect the security of information conducted in this research has revealed the impossibility of ensuring for the level of models of invulnerability of processing technology and information transfer using flexible protective mechanisms, due to the lack of integration of mathematical models of the processing and protection of information [8, 12, 17, 20].

MATERIALS AND METHODS

Any model of the security policy (SP) to ensure the HRIP necessarily support the global SP characterizing the desired properties of IP (access syntax), and can support the local SP, which characterizes the transition rules of IP between the neighboring states (the semantics of access). Availability of support the local SP means dynamics of the appropriate model, and absence means the static. The dynamic model of SP, as opposed to static, imposes constraints on the state of IP [6, 10, 15, 22].

If the set of possible states of the automated data processing systems of critical applications (ADPS CA) can be represented as a finite set, then the model of SP refers to the class of finite state models. The theoretical basis of the fundamental security of such models of SP is the so-called fundamental theorem of security, which is stated and proved separately for every model [7, 19, 28, 29]. According to it if at the initial time the global SP is performed and all the transitions of IP from state to state fulfill the corresponding local SP, then at any time thereafter, the global SP will also be performed. Therefore, vulnerabilities of IP of this type are not directly incorporated into the model of SP, but must occur only in practical realization [18, 21].

The discretionary model, setting access permissions of users, in general, acting in certain roles, to objects, no operating with transitions between IP, most perfectly supports the global SP. However, not be referring to the model of the final states, it is not fundamentally safe.

In this regard, the topical problem is the development of models of SP complexes, which are models of the final states in substance and discretionary in form. The formalism of such models should integrate graph-theoretic basis of discretionary formalism, static in nature, and convenient to describe the information processes, network formalism, having a dynamic character. As a result, it should describe by uniform way the dynamic and static access to information, structured to ensure the unity of the local and global SP review.

In terms of confidentiality and availability of information protection mechanisms flexibility refers to the flexibility of differentiation of access and the vulnerability is embedded in the model used by SP and its practical implementation. The only truly flexible is discretionary model of SP, which inevitably creates vulnerabilities. On the other side, the only intrinsically safe is the class of models of the final states, originating from the mandatory access control method. However, the application of existing models of the final states is very limited due to their principal inflexibility [17, 25, 26]. This disadvantage of this class of models can be eliminated, brought closer together this class of models with the discretionary model. Nevertheless, it is hampered by the conventional independent review of processes to protect information from its processing, and retreat from this principle requires new research, the results of which are presented in this work.

The reason lies in the fundamental theoretical difficulties of modeling technologies ensuring the reliability and protection of IP in automated data processing systems of critical applications (ADPS CA) occurring when you try to connect a promising approach to ensure the safety and protection of IP from UA with the flexibility of the protective mechanisms [3, 8, 14, 29].

RESULTS OF RESEARCH

The analysis of existing methods of modeling processes HRIP in ADPS affecting the security of the information has allowed to choose basic graph-theoretic modeling unit of IP protection from UA in ADPS SP - E-networks unit.

The automated systems on transport vary in technologies applied, from basic management systems such as car navigation, traffic signal control systems, container management systems, variable message signs, automatic number plate recognition or speed cameras to monitor applications, such as security CCTV systems, and to more advanced applications that integrate live data and feedback from a number of other sources, such as parking guidance and information systems, weather information, and the like.

A Transportation Management System (TMS) is a software system designed to manage transportation operations. TMS are one of the systems managing the supply chain. They belong to a sub-group called Supply chain execution (SCE). TMS, whether it is part of an Enterprise Level ERP System and has become a critical part of any (SCE).

The block diagram of a typical control system for transport is shown in Fig. 1.

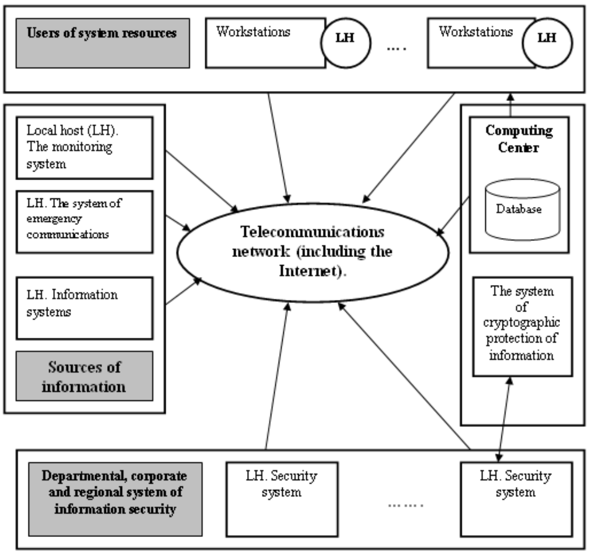

Users of system resources
Workstations
LH
....
Workstations
LH
Local host (LH). The monitoring system
LH. The system of emergency communications
LH. Information systems
Sources of information
Telecommunications network (including the Internet).
Computing Center
Database
The system of cryptographic protection of information
Departmental, corporate and regional system of information security
LH. Security system
....
LH. Security system

Fig. 1. The block diagram of control system for transport

Rapidly changing external and internal business environment, necessity to adapt oneself very quickly and take adequate management decisions in time make the effective use of corporate information to be a pre-requisite for business success.

Based on the analysis in the works [14, 17, 29], the purpose and objectives of the research are defined. According to the proposed system approach, the main result of the formation of methodological bases of safety and reliability of IP in ADPS SP is a reference model of secure automated system (RMSAS) as an idealized model of ADPS SP implementing fundamentally safe technology of information circulation. Such model allows standardization of unified architectural appearance of different classes of ADPS SP by developing and registering for the regulation of safety standards. Regulated reference models of secure automated system (RMSAS models) of complexes of SP, joining the existing model of the final states with discretionary form, provide that any discretionary access can be realized only by uniquely defined sequence of transitions between the end states for which one can guarantee its safety.

However, due to the specificity of IP in the reference ADPS, the direct use for it such general formalisms inherent for E-networks is little effective [14]. Therefore, based on the E-networks unit has been built a new graph-theoretic unit of problem-oriented nature – RMSAS networks. Relying of an equivalent E-network representation, a proper specific syntactic representation of RMSAS networks by minimizing the descriptive means has been found – the canonical form of RMSAS network.

The composition of RMSAS network is defined as follows:

L – number of RMSAS network levels (usually L=13), $k=\overline{1,L}$, $l=\overline{1,L}$, $k \neq l$, S – positions quantity, $S = Q \cup P \neq \emptyset$, $Q \cap P = \emptyset$, $|S| < \infty$, $|Q| = |P|$, Q, P – quantities of simple and permissive positions, $|Q| < \infty$, $|P| < \infty$, $Q = \bigcup_{l=1}^{L} Q_l \neq \emptyset$, $Q_k \cap Q_l = \emptyset$,

$P=\bigcup_{l=1}^{L} P_l \neq \varnothing$, $P_k \cap P_l = \varnothing$, Q_l, P_l – quantities of simple and permissive positions of the l-st level, $|Q_l| = |P_l| \neq 0$, U – quantity of modules, $U=\bigcup_{l=1}^{L} U_l \neq \varnothing$, $|U| < \infty$, $U_k \cap U_l = \varnothing$, U_l – quantity of modules of the l-st level, $I(u) = i_1.i_2.....i_{L-l}$ – index module $u \in U_l$ and unit, which this module is the upper (№ 0 in the unit), particularly, $I(u)=0$ when $l=L$, $K[I]$ – number of the lower modules in unit with index I, $I.j$ – index of the lowest module with number $j=\overline{1,K[I]}$ in the unit with index I, if I, J – module indexes, than:

$$(J \subset I) \Leftrightarrow (I \supset J) \Leftrightarrow (I = J.i_1.i_2....i_k),$$

$$(J \subseteq I) \Leftrightarrow (I \supseteq J) \Leftrightarrow ((J \subset I) \vee (I = J)).$$

To specify the structure of the RMSAS network we introduce the notation: N – quantity of number of authorization, $\alpha=\overline{1,N}$ – number of authorization, $r=r[I,\alpha]$ – Boolean attribute of the admissibility of authorization α in the module with index I, $M_{in}=M_{in}[I,\alpha]$, $M_{\text{out}}=M_{\text{out}}[I,\alpha]$ – input and output functions of marking defining marking of input and output modules positions in form of a Boolean variable (indicate whether the position of the chip, and each item can contain no more than one chip).

The formal presentation of the RMSAS network module of given structure looks like:

$$u=\langle I, q=q[I,\alpha], p=p[I,\alpha]\rangle \in U_l, \quad (1)$$

where: $I=I(u)$ – index of module, $q=q[I,\alpha]\in Q_l$, $p=p[I,\alpha]\in P_l$.

Moreover, the formal representation of the structure of the network RMSAS is the next:

$$\varepsilon=\left\langle \begin{matrix} N, K=K[I], r=r[I,\alpha], \\ M_{in}=M_{in}[I,\alpha], M_{\text{out}}=M_{\text{out}}[I,\alpha] \end{matrix} \right\rangle. \quad (2)$$

Bringing into service of RMSAS networks opens the way for a systematic research of its mathematical properties as a development tool of ADPS CA based on the RMSAS. A fundamental step in this direction is the construction of using the unit of RMSAS networks modeling approach complex SP of the reference ADPS in the form of SP of RMSAS network.

Global (g) SP and discretionary of the l-st level are given as set of allowed positions: $\Psi_{\text{g}} \subseteq P_I$, $\Psi_{dl} \subseteq P_l$, and leveled structure (l) looks like:

$$\Psi_{ll}=\left\{ \begin{matrix} \langle I(u), \alpha, r[I(u),\alpha]\rangle | u \in \\ U_l, \alpha=\overline{1,N} \end{matrix} \right\}. \quad (3)$$

Block SP (b) is given by the installation of admissibility of evidence of various authorizations in all modules of the block, agreed to the following rules ($\alpha=\overline{1,N}$, $I=I(u)$, $u \in U \setminus U_1$):

$$\begin{aligned} &(\exists_j \in \overline{1,K[I]})(r[I.j,\alpha]=1) \Rightarrow \\ &\Rightarrow (r[I,\alpha]=1), \end{aligned} \quad (4)$$

$$\begin{aligned} &(r[I,\alpha]=0) \Rightarrow \\ &\Rightarrow (\forall_j \in \overline{1,K[I]})(r[I.j,\alpha]=0). \end{aligned} \quad (5)$$

Local SP is given as follows:

$$\Psi_1=\bigcup_{l=1}^{L}\Psi_{ll}=\left\{ \begin{matrix} \langle I(u), \alpha, r[I(u),\alpha]\rangle | u \in \\ U, \alpha=\overline{1,N} \end{matrix} \right\}, \quad (6)$$

where: all $r[I(u),\alpha]$ are mutually agreed to all blocks in accordance with the rules:

$$(\alpha=\overline{1,N},\ I-I(u)):$$

$$\begin{aligned} &(r[I,\alpha]=1) \Rightarrow (\forall J \subset I)(r[J,\alpha]=1), \\ &u \in U \setminus U_L, \end{aligned} \quad (7)$$

$$(r[I,\alpha]=0)\Rightarrow(\forall J\supset I)(r[J,\alpha]=0),\quad u\in U\setminus U_1. \tag{8}$$

Discretionary SP is given by its permissive $\Psi_{\partial p}$ or globalized $\Psi_{\partial g}$ representation:

$$(p[I,\alpha]\in\Psi_{\partial g})\Leftrightarrow((p[I,\alpha]\in\Psi_{\partial p})\wedge \wedge(\forall J\supset I)(p[J,\alpha]\notin\Psi_{\partial p}));$$

$$\Psi_{\partial p}=\bigcup_{l=1}^{L}\Psi_{\partial l}\subseteq P,\ \Psi_{\partial g}\subseteq\Psi_{\partial p},\ \alpha=\overline{1,N},\quad I=I(u),\ u\in U, \tag{9}$$

besides the quantities $\Psi_{\partial l}$ are agreed to rule ($\alpha=\overline{1,N}$):

$$(p[I,\alpha]\in\Psi_{\partial p})\Rightarrow \Rightarrow(\forall J\subset I)(p[J,\alpha]\in\Psi_{\partial p}),\quad I=I(u),\ u\in U\setminus U_L, \tag{10}$$

$$(p[I,\alpha]\notin\Psi_{\partial p})\Rightarrow \Rightarrow(\forall J\supset I)(p[J,\alpha]\notin\Psi_{\partial p}),\quad I=I(u),\ u\in U\setminus U_1. \tag{11}$$

The induction of discretionary global security policy means $\Psi_g=\Psi_{\partial g}$, and the local security policy of discretionary means –

$$(\forall p=p[I,\alpha]\in P)((p\in\Psi_{\partial p})\Leftrightarrow \Leftrightarrow(r[I,\alpha]=1)). \tag{12}$$

During researches have been developed mathematical models of the synthesis of secure communications policy interaction of the reference ADPS that can consider SP of some IP (at different structural components RMSAS-network) with the possibility of further interlinkages (a layered synthesis of SP on RMSAS network). As the basic structural components have been defined in a network interpretation (as part of RMSAS network) and systemic treatment (as appropriate system quantities) layers and concepts of superblock of RMSAS network. The layer $S_{lH\ldots lb}$ of the level l_b with the lowest level l_H of RMSAS network $B_0=S_{1\ldots L}$ is (in the network interpretation) part of RMSAS network related to the levels of RMSAS with numbers $l=\overline{l_H,l_{\text{в}}}$.

Superblock $S_{lH\ldots lb}(I)$ of the level l_H with the index I (given superblock of RMSAS network $S_{lH\ldots lb}$) of RMSAS network $B_0=B_{1\ldots L}(0)$ is a part of layer $S_{lH\ldots lb}$ with moduls index $J\subseteq I$. The ways setting various SP on individual structural components of RMSAS network, in particular, its layers and superblocks, by analogy with the task SP in all RMSAS network are identified.

For the account of the possibility of SP interlinkages given on the various structural components of RMSAS network, the concept of SP compatibility in two different senses is formally defined for all pairs of types of SP. Weak compatibility of random SP Ψ_1 and Ψ_2, denoted as $\Psi_1\sim\Psi_2$ is the lack of direct conflict between them. Strong compatibility of random SP Ψ_1 and Ψ_2, denoted as $\Psi_1\approx\Psi_2$ is the inability of a conflict between them, even in distributing of SP to all RMSAS network.

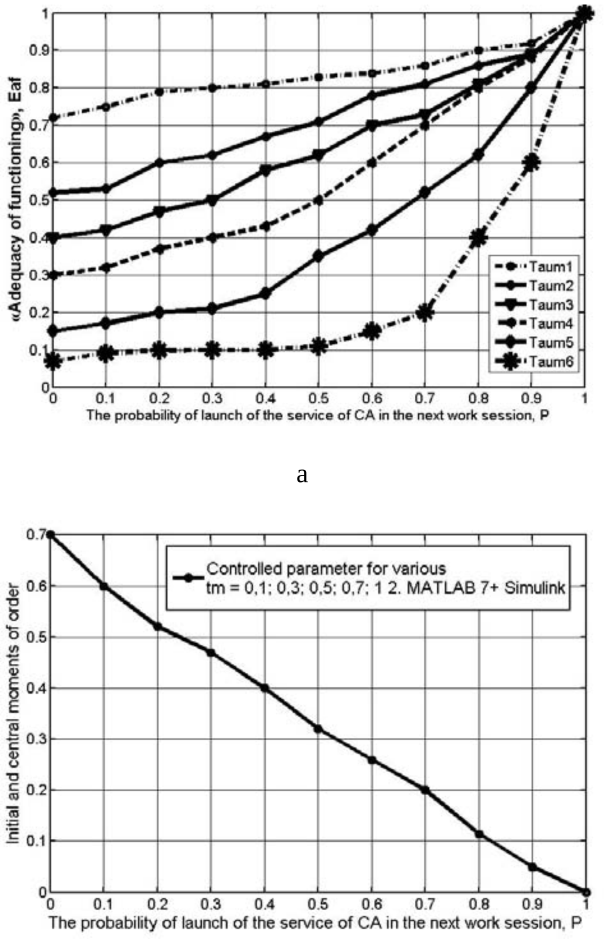
A set of criteria quality of service operation of CA as a control object has been substantiated:

1) dynamic – «adequacy of functioning» E_{af}, «temporary aggressiveness of functioning» E_{ta},

2) static (Boolean) – «functionality» E_f, «resource aggressiveness of functioning» E_{ra}, «functional aggressiveness of functioning» E_{fa}, «usability» E_{yu}.

In the MatLab and DELPHI programming environment we created a complex of problem-oriented software for modeling service management of CA of information processed as in conventional so in reference ADPS. It, in particular, allows us to construct graphic dependences of dynamic criteria, regardless of the variable parameters. Using these graphics choosing the optimal values of the controlled parameters and evaluate the attainable level of targets is visualized.

With the help of the developed software has been conducted a comprehensive research of the quality of the functioning of typical SIP as applied to the operation of workstations based on computers as part of ADPS and the criteria of efficiency and dynamic characteristics of the lifetime of the FSP (time of CA using discretionary access) in the reference ADPS (Fig. 2).



a

b

Fig. 2. The results of the calculations for the reference ADPS:
a – criteria of dynamic efficiency,
b – mathematical expectation.

For the reference ADPS the results of calculations were presented in the form of dependencies of output variables from the single (unique for each method), regardless of the varied managed parameter by different $\tau_m = 0{,}1;0{,}3;0{,}5;0{,}7;1;2$ (curves *taumi*, $i = \overline{1{,}6}$) and a different number of controlled levels $l_{\max} = 1;3;6;9;12;15$ (curves *lmaxai*, $i = \overline{1{,}6}$).

The data mining process effectively reduces the size of the data that needs to be retained for future comparisons. The network data processor (NDP) prepares counts and other statistical measures from the mined data and stores them to disk. Since FIRE is an anomaly detection system, the measures are chosen such that anomalies in network data can be ascertained easily.

Typical summaries include:

1. The number of total packets observed in the data collection interval.

2. The number of unique sdp’s observed in the interval.

3. The number of sdp’s that are new in this data collection interval.

4. The number of sdp’s that are new in the longerterm data retention interval (i.e. have never been seen before).

5. The number of well-known ports used in an interval.

6. The variance of the count of packets seen against the sdp’s.

7. The number of sdp’s that include foreign hosts (hosts outside the local network domain).

8. The number of successfully established TCP connections in a time interval.

Analytical model of membership function of variable ϕ (ϕ – controlled input variables) to an arbitrary fuzzy term T can be expressed as

$$\mu^T(\phi) = \frac{1}{1 + \left(\dfrac{\phi - \alpha}{\beta}\right)^2}, \qquad (13)$$

where: α – coordinate of the maximum function, β – the coefficient functions.

Function of the controlled parameter ϕ_i fuzzy set of values conducive to the realization of the *j*-th option, describe the function (*S*-*Q*)-type:

$$\mu_j(\phi_i) = \begin{cases} S\left(\dfrac{\phi_i - \overset{0\,j}{\phi_i}}{\varsigma_{ij}}\right), \phi_i \le \overset{0\,j}{\phi_i}, \\ Q\left(\dfrac{\phi_i - \overset{0\,j}{\phi_i}}{\xi_{ij}}\right), \phi_i > \overset{0\,j}{\phi_i}, \end{cases} \tag{14}$$

where: S and Q arbitrary functions that do not grow on the set of positive real numbers, $\varsigma > 0$, $\xi > 0$ (Options ς and ξ are respectively the left and right fuzziness coefficients),

Membership function in terms of (S-Q) correlation functions will be described:

$$\mu(\phi) = \begin{cases} \dfrac{1}{1 + \left(\dfrac{\alpha - \phi}{\beta}\right)^2}, & \phi \le \alpha, \\ \dfrac{1}{1 + \left(\dfrac{\phi - \alpha}{\beta}\right)^2}, & \phi > \alpha. \end{cases} \tag{15}$$

FIRE consists of the three types of components: network data collector (NDC), network data processor (NDP), Fuzzy Threat Analyzer (FTA). The network data collector (NDC) is a promiscuous network data sniffer and recorder. It reads raw network packets off the wire and stores them on disk. The next component, the network data processor (NDP), summarizes and tabulates the raw packet data in carefully selected categories. In a sense, an NDP performs a kind of data mining on the collected packets. The NDP merges these summaries and tables with past data and stores them on disk. Next, the NDP compares the current data with the historical mined data to create values that reflect how the new data differs from what was observed in the past. These values are “fuzzified” to produce the fuzzy inputs needed by the Fuzzy Threat Analyzer (FTA). The resulting fuzzy inputs from the NDPs are called “fuzzy alerts” because they represent an alert condition to a degree.

Example list of factors that affect the productivity of information systems under the threat of DDoS attacks, presented in the form of linguistic variables, for which the selected set and universal terms. According constructed fuzzy knowledge base, representing a set of fuzzy rules "IF-THEN" that define the relationship between input and output variables. For fuzzy knowledge bases composed logical equation:

$$\mu^{d_j}(D) = \bigvee_{p=1}^{h_j} \begin{bmatrix} \mu^{y_3^{jp}}(y_3) \wedge \mu^{y_4^{jp}}(y_4) \wedge \cdots \\ \wedge\, \mu^{\phi_z^{jp}}(\phi_z) \end{bmatrix}, \tag{16}$$

$$p = \overline{1, h_j}\,,\; j = \overline{1, U}.$$

Once the NDP completes the data mining phase, it produces fuzzy sets based on past input data. FIRE uses the historical and statistical data for each element of matrix (Eq. 17). We have arbitrarily chosen five fuzzy sets for each data element: low, medium-low, medium, medium-high, and high (Table 1). By standardizing the number of sets, we can apply the same fuzzy rules against the data from each NDP, regardless of the differences in the local input domain.

$$H = \begin{pmatrix} \phi_{11} & \phi_{12} & \cdots & \phi_{1i} & \cdots & \phi_{1n} \\ \phi_{21} & \phi_{22} & \cdots & \phi_{2i} & \cdots & \phi_{2n} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \phi_{l1} & \phi_{l2} & \cdots & \phi_{li} & \cdots & \phi_{ln} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \phi_{N1} & \phi_{N2} & \cdots & \phi_{Ni} & \cdots & \phi_{Nn} \end{pmatrix}. \tag{17}$$

In a common intrusion scenario, an attacker conducts a port scan of a network, sending packets to several well-known ports (FTP, HTTP, etc.) looking for systems that might be running those services. The presence of those services on a system gives a hint as to what vulnerabilities the attacker might try to exploit to penetrate the system. Additionally, the attacker may use scanners that can accurately identify the operating system on the target machine by examining the response of the TCP stack to carefully crafted TCP control messages.

Table 1. Factors affecting the productivity of information systems for DDoS and DoS attacks

A partial state variable of the information system and Network	**Univer-sum**	Terms for lingu-istic asses-sment
ϕ_1 – indicator of current risks [10]	[0,1], arbitrary units (A.U.).	*low*, *medium-low*, *medium*, *medium-high*, and *high*
ϕ_2 – acceptable level of risk information	[0,1], A.U.	-
ϕ_3 – intensity of flow rate (requests) coming to servers	[10,6000], frame / s	-
ϕ_4 – nominal capacity of the environment data	[10,100], Mbit / s	-
ϕ_5 – number of attempts to access to environmental data generated by an attacker to view	$[0, \mathrm{N}_a]$	-
ϕ_6 – the service transaction	[0,001-0,01], s	-
ϕ_7 – IP pocket length	[1 -65529], byte	-
ϕ_8 – large number of IP packets with the type of attack Ping of Death	[0,1], A.U.	-
ϕ_9 – number of http-requests to the object of attack	[0,1], A.U.	-
ϕ_{10} – presence of TCP packets	[0,1], A.U.	-
ϕ_{11}– presence of UDP packets	[0,1], A.U.	-
ϕ_{12} – presence of ICMP packets	[0,1], A.U.	-
ϕ_{13}– availability of SQL injection	[0,1], A.U.	-
ϕ_{14} – interval between frames	[10-100], bit	-
…		-
ϕ_z – other factors		-

Knowledge of the services running and the host operating system is extremely valuable to the attacker because it helps to narrow the types of vulnerabilities the attacker can exploit on the systems. Port and operating system detection scanning may be a strong indicator that a more serious attack may be occurring in the future.

With the fuzzy input sets defined, the security administrator can then construct the rules of the fuzzy system. Fuzzy rules are written using common sense experiences by the security administrator. The rules designer seeks to define rules that cover as much of the input space as possible Using tools such as the Matlab Fuzzy Toolbox, the designer can check the input rule space to ensure that the fuzzy rules cover the input space and that all output responses are defined (Fig. 3).

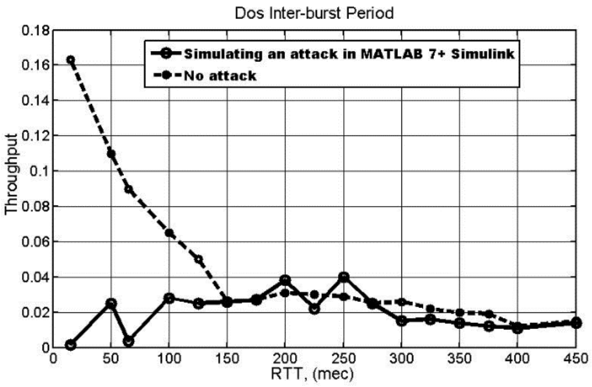


Fig. 3. Dos Inter-burst Period

DISCUSSION

Analysis of the results of calculations, part of which is shown in Fig. 2, 3 allows you to identify patterns of governance. They do not contradict the known data and show the opportunities of modeling.

A task-oriented graph-theoretic unit of RMSAS networks, allowing to model invulnerable processing and transmission of information with flexible protective mechanisms, providing a formalization and research of RMSAS SP is developed. It uses not only the details of the transfer process, but the data within the proposed hierarchical structuring of RMSAS resources for unified modeling of dynamic and static information access based on the integration of E-network and discretionary formalisms.

A method for modeling RMSAS networks regulated RMSAS SP for HRIP, allowing combining the flexibility of discretionary models with security of models of the final SP states is developed.

CONCLUSION

Thus, studies with the following results.

1. A task-oriented graph-theoretic unit of RMSAS networks, allowing to model invulnerable processing and transmission of information with flexible protective mechanisms, providing a formalization and research of RMSAS SP is developed. It uses not only the details of the transfer process, but the data within the proposed hierarchical structuring of RMSAS resources for unified modeling of dynamic and static information access based on the integration of E-network and discretionary formalisms.

2. Mathematical models and algorithms of optimal control of the integrity of information processed, while maintaining the effectiveness of this treatment, allowing us to find a compromise between ensuring the integrity and the efficiency of information processing are developed.

3. Exact analytical method for evaluating and analysis of the complex criteria for assessing the quality service operation of CA of information uses semi-Markov matrix formalism, integrating matrix formalism of finite Markov chains and operator formalism of random processes in a single review of continuous-time and discrete states.

REFERENCES

1. **Ahmad D., Dubrovskiy A., Flinn X., 2005.:** Defense from the hackers of corporate networks. Trudged. with angl. – 2th izd. M.: Companies AyTi, DMK - Press. 864. (in Russian).
2. **Atighetchi M., Pal P., Webber F., Schantz R., Jones C., Loyall J., 2004.:** Adaptive Cyberdefense for Survival and Intrusion Tolerance // Internet Computing. Vol. 8, No.6. – 25-33.
3. **Atighetchi M., Pal P.P., Jones C.C., Rubel P., Schantz R.E., Loyall J.P., Zinky J.A., 2003.:** Building Auto-Adaptive Distributed Applications: The QuO-APOD Experience // Proceedings of 3rd International Workshop Distributed Auto-adaptive and Reconfigurable Systems (DARES). Providence, Rhode Island, USA. 74-84.
4. **Chapman C., Ward S., 2003.:** Project Risk Management: processes, techniques and insights. Chichester, John Wiley. Vol. 1210.
5. **Chertov R., Fahmy S., Shroff N., 2006.:** Emulation versus simulation: A case study of TCP-targeted denial of service attacks. In Proc. of the 2nd International conference on Testbeds and Research Infrastructures for the Development of Networks and Communities.
6. **Chi S., Park J., Jung K., Lee J., 2001.:** Network Security Modeling and Cyber At-tack Simulation Methodology//LNCS. Vol. 2119.
7. **Goldman R., 2002.:** A Stochastic Model for Intrusions//LNCS. Vol. 2516.
8. **Gorodetski V., Kotenko I., 2002.:** Attacks against Computer Network: Formal Grammar-based Framework and Simulation Tool. RAID 2000//LNCS. Vol. 2516.
9. **Harel D. Statecharts: A., 1987.:** Visual Formalism for Complex Systems, Science of Computer Programming.
10. **Hariri S., Qu G., Dharmagadda T., Ramkishore M., Raghavendra C., 2003.:** Impact Analysis of Faults and Attacks in Large-Scale Networks//IEEE Security & Privacy. 456-459.
11. **Hatley D., Pirbhai I., 1988.:** Strategies for Real-Time System Specification, Dorset House Publishing Co., Inc., NY.
12. **Keromytis A., Parekh J., Gross P., Kaiser G., Misra V., Nieh J., Rubensteiny D., Stolfo S., 2003.:** A Holistic Approach to Service Survivability // Proceedings of ACM Workshop on Survivable and Self-Regenerative Systems. Fairfax, VA. 11-22.
13. **Larson D.R., Field W.E., Farahmand F., Jeffries J.L., 2006.:** Foundations in Homeland Security Studies. Purdue University.
14. **Larson D.R., Field W.E., F. Farahmand, Aaltonen P.M., 2007.:** Managing Resources and Applications for Homeland Security. Purdue University.
15. **Lufar V., 2012.:** Database of hazardous substances properties. TEKA Commission of Motorization and Power Industry in Agriculture, V. XII, No. 3, 90-93.
16. **Marcus K., Mcquade S. 2011.:** Internet Addiction and Online Gaming (Cybersafety). Chelsea House Pub.
17. **Marcus K., Mcquade S. 2011.:** Living With the Internet (Cybersafety). Chelsea House Pub.
18. **McNab C., 2004.:** Network Security Assessment. O’Reilly Media, Inc.
19. **Mirkovic J., Dietrich S., Dittrich D., Reiher P., 2004.:** Internet Denial of Service: Attack and Defense Mechanisms. Prentice Hall PTR, 400.
20. **Moitra S. D., Konda S. L., 2000.:** A Simulation Model for Managing Survivability of Net-worked Information Systems, Technical Report CMU/SEI-2000-TR-020.
21. **Negoita M., Neagu D., Palade V., 2005.:** Computational Intelligence Engineering of Hybrid Systems. Springer Verlag. 213.
22. **Piszcz A., Orlans N., Eyler-Walker Z., Moore D., 2001.:** Engineering Issues for an Adaptive Defense Network. MITRE Technical Report.

23. **Rohse M., 2003.:** Vulnerability naming schemes and description languages: CVE, Bugtraq, AVDL and VulnXML. SANS GSEC PRACTICAL.
24. **Smirniy M., Lahno V., Petrov A., 2009.:** The research of the conflict request threads in the data protection systems. Proceedings of Lugansk branch of the International Academy of Informatization. № 2(20). V 2. 2009. – 23-30.
25. **Shun-Chieh Lin & Shian-Shyong Tseng. 2004.:** Constructing detection knowledge for DDoS intrusion tolerance // Expert Systems with Applications. – 2004. – Vol. 27. – 379-390
26. **Templeton S., Levitt K., 2000.:** A Requires/Provides Model for Computer Attacks. Proc. of the New Security Paradigms Workshop. 274-280.
27. **Xiang Y., Zhou W., Chowdhury M., 2004.:** A Survey of Active and Passive Defence Mechanisms against DDoS Attacks. Technical Report, TR C04/02, School of Information Technology, Deakin University, Australia. 38-43.
28. **Slobodyanuk M., Nechaev G., 2010.:** The evaluation technique of logistics system cargo ransportation efficiency development.TEKA Kom. Mot I Energ. Roln. – OL PAN, 10B. Lublin, 162-170.
29. **Urgen M.W. Pan and S. Stolfo., 2002.:** Ensemble-based adaptive intrusion detection. In Proceeding of 2002 SIAM International Conference on Data Mining, Arlington, VA.
30. **White D., Alijani G., 2003.:** Identifying requirements for network security software. SAM ’03. International Conference, 539-543.
31. **Zou C.C., Duffield N., Towsley D., Gong W., 2006.:** Adaptive Defense against Various Network Attacks // IEEE Journal on Selected Areas in Communications: High-Speed Network Security (J-SAC). Vol.24, №.10. – 44 -51.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КРИТИЧЕСКИ ВАЖНЫХ СИСТЕМ ОБРАБОТКИ ИНФОРМАЦИИ

Валерий Лахно

Аннотация. Статья содержит результаты исследований, позволяющие повысить уровень защиты автоматизированных и интеллектуальных информационных систем предприятий и компаний. В статье предложен проблемно-ориентированный теоретико-графовый аппарат эталонных моделей защиты автоматизированных систем, позволяющий моделировать неуязвимые технологии обработки и передачи информации. Предлагаемый в работе системный подход для решения задач информационной безопасности, предусматривает интеграцию математических моделей обработки и защиты информации, соединяющий неуязвимость и гибкость по каждому из трех аспектов защищенности (конфиденциальность, доступность и целостность) информации на основе конструктивной унификации указанных противоречий. Разработан метод моделирования политики безопасности (ПБ) для обеспечения высоконадежной обработки информации (ВНОИ), отличающийся использованием нового проблемно-ориентированного теоретико - графового аппарата эталонной модели защищенной автоматизированной системы для соединения гибкости дискреционной модели с принципиальной безопасностью моделей конечных состояний ПБ.

Ключевые слова: информационная безопасность, автоматизированная система, политика безопасности, математические модели.