MEST JOURNAL
DOI 10.12709/mest.02.02.01.07

ENSURING OF INFORMATION PROCESSES' RELIABILITY AND SECURITY IN CRITICAL APPLICATION DATA PROCESSING SYSTEMS

Valery Lahno
Lugansk National Agrarian University, Lugansk, Ukraine

JEL category: **M15, O31**

Summary:
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. This model connects invulnerability and flexibility for each of three aspects of security (confidentiality, availability and integrity) of information based on structural unification of these contradictions. The method of modeling the security policy (SP) to provide a highly reliable information processing (HRIP) has been developed. This method differs by using a new problem-based graph-theoretic unit of standard model of the protected automated system for connection flexibility the discretionary model with the principled security of models of the final states of the SP. 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.

Keywords:
protection of information, data processing system, security policy, mathematical model, reliability

The address of the author:
Valery Lahno
lva964@gmail.com

1 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 (Ahmad, Dubrovskiy, & Flinn, 2005).

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

This eliminates a number of inconsistencies in the definition of conflict MIP and attack.

In so doing, the reliability of IP should be characterized by its conformity to some reference security model (invincible) circulation (processing and transmission) of information. In this regard, there is a practical problem that such things are only partially implemented in practice and is not directly reflected in the relevant standards for architectural solutions of automated systems, such as transport satisfying the common reference models (Lahno & Petrov, 2010).

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.

It should be noted that the ADPS CA are the result of the introduction of computer technology in the field of critical objects (military sites, environmentally dangerous production, nuclear power plants, objects of transport, communication, financial and credit sector, etc.), which are characterized as not acceptable to society damages for breach their performance. In ADPS CA, reliability of IP overrides its functionality. Moreover, it is preferred to use perspective approach (Chi, Park, Jung, & Lee, 2001).

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.

2 FORMULATION OF THE RESEARCH PROBLEMS

The objects of the study, the results of which are presented in this article are HRIP processes with flexible protective mechanisms. The subjects of the study are methods and process models HRIP to ensure the prevention of its vulnerabilities against threats of intentional and unintentional nature and flexibility of the defense mechanisms.

The purpose of the study is the development of the theoretical foundations of HRIP process modeling providing both preventing its vulnerabilities against threats of intentional and unintentional nature and flexibility of defense mechanisms by integrating mathematical models of the information processing and protection.

This purpose required the solution of the following tasks:

- development of mathematical models of flexible accessibility, confidentiality and integrity of processed information;
- development of mathematical models and algorithms for optimal control of the integrity of processed information, while maintaining the effectiveness of this processing;
- development of a complex of problem-oriented programs of quality complex estimation of service operation of IC information.

2.1 Previous researches

In works (Ahmad, Dubrovskiy, & Flinn, 2005) the ways of HRIP improvement and enhance the protection of IP in ADPS CA. Depending on what system information considered IP flow, the modern approach to ensure their safety and

reliability is satisfied to a greater or lesser extent. A striking example of the weak satisfactory give ADPS CA on transport (Lahno & Petrov, 2011), and on this basis we shall discuss IP here.

Analysis of advanced technologies HRIP in the ADPS showed that prospective ADPS CA must use an object-relational database management system (DBMS). The relational data model as a theoretical basis of functionality of perspective object-relational DBMS CA together with associated models of information processing should be integrated with the advanced models of SP in a joint gauge model of safe circulation of information in the ADPS SP. Analysis of the existing approaches to the construction of systems of information protection from UA (SIP UA) in ADPS CA has shown that the use of traditional stand-alone SIP with the pursuit of their universality, in accordance with the concept of a padlock contradicts the prospective approach to ensuring the reliability and security of IP. The modern approach based on SIP UA satisfying protection profiles and security tasks, reflecting the possibility of countering known threats, to overcome a number of inconsistencies in the definition of confrontation means of defense and attack.

2.2 Management of information security

Analysis of existing methods of organizing process management of IP protection from UA to ADPS SP showed relevance of the task of organizational and technological service management of IC (Shun-Chieh & Shian-Shyong, 2004). It represents a problem of optimal control of IC service by automating its launch on performance criteria, providing the best IC while maintaining efficient operation of ADPS CA. However, this automation remains a problem even for those used in modern ADPS typical SIP UA. The analysis of the standardized evaluation method of the quality and efficiency of security systems services (SSS) as the software (SW) in relation to the specifics of organization of service management IC in ADPS SP showed the inadequacy of the characteristics of the properties of the service provided by IC as a control object. Therefore, it is suggested to introduce new features and sub characteristics – the criteria of quality of service operation IC as a control object.

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.

Based on the analysis in the works (Harel, 1987; Ahmad, Dubrovskiy, & Flinn, 2005), 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.

3 ENSURING OF INFORMATION PROCESSES' SAFETY AND SECURITY IN CRITICAL APPLICATION DATA PROCESSING SYSTEMS

For the mathematical modeling of IP in ADPS, it is offered its formal representation by a known device of E-networks created in the development of the now-classic unit of Petri nets.

It develops the traditional graph formalization in the field by introducing a standard for the E-network unit of time delay procedures and permitting procedures. E-network representation of the dynamics of functioning in a typical MIP UA in normal ADPS CA and functioning of the IP dynamics in the reference ADPS has been developed (Harel, 1987).

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 (Smirniy M. & Lahno V., 2009). 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, $S=Q\cup P\neq\varnothing$, $Q\cap P=\varnothing$, $|S|<\infty$, $|Q|=|P|$;

Q, P – quantities of simple and permissive positions, $|Q|<\infty$, $|P|<\infty$, $Q=\bigcup_{l=1}^{L}Q_l\neq\varnothing$, $Q_k\cap Q_l=\varnothing$, $P=\bigcup_{l=1}^{L}P_l\neq\varnothing$, $P_k\cap P_l=\varnothing$;

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:

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

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: $\Psi_g\subseteq P_I$; $\Psi_{dl}\subseteq P_l$, 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 installation of admissibility of evidence of various authorizations in all modules of the block, agreed to the following rules ($\alpha=\overline{1,N}$, $I=I(u)$, $u\in U\setminus U_1$):

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

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

Local SP is given as follows:

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

where all $r\left[I(u), \alpha\right]$ are mutually agreed to all blocks in accordance with the rules ($\alpha = \overline{1, N}$, $I - I(u)$):

$$(r\left[I, \alpha\right] = 1) \Rightarrow (\forall J \subset I)(r\left[J, \alpha\right] = 1), \\ u \in U \setminus U_L; \quad (7)$$

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

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

$$(p\left[I, \alpha\right] \in \Psi_{\ddot{a}\eth}) \Leftrightarrow ((p\left[I, \alpha\right] \in \Psi_{\ddot{a}\eth}) \wedge \\ \wedge (\forall J \supset I)(p\left[J, \alpha\right] \notin \Psi_{\ddot{a}\eth}));$$

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

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

$$(p\left[I, \alpha\right] \in \Psi_{\ddot{a}\eth}) \Rightarrow \\ \Rightarrow (\forall J \subset I)(p\left[J, \alpha\right] \in \Psi_{\ddot{a}\eth})'$$

$$I = I(u), \; u \in U \setminus U_L; \quad (10)$$

$$(p\left[I, \alpha\right] \notin \Psi_{\ddot{a}\eth}) \Rightarrow \\ \Rightarrow (\forall J \supset I)(p\left[J, \alpha\right] \notin \Psi_{\ddot{a}\eth})'$$

$$I = I(u), \; u \in U \setminus U_1. \quad (11)$$

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

$$(\forall p = p\left[I, \alpha\right] \in P)((p \in \Psi_{\ddot{a}\eth}) \Leftrightarrow \\ \Leftrightarrow (r\left[I, \alpha\right] = 1)). \quad (12)$$

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 $S_{l_H \ldots l_в}$ of the level $l_в$ 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 $l = \overline{l_H, l_в}$.

Superblock $S_{l_H \ldots l_в}(l)$ of the level l_H with the index l (given superblock of RMSAS network $S_{l_H \ldots l_в}$) of RMSAS network $B_0 = B_{1\ldots L}(0)$ is a part of layer $S_{l_H \ldots l_в}$ 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.

During the research is made a modeling of organizational and technological CA service management in case of IP protection of the typical SIP UA and in case of the reference ADPS. In both cases, for supporting the adoption of appropriate information security manager solutions it is proposed to use the new subsystem - the automated service management subsystem of information CA.

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}.

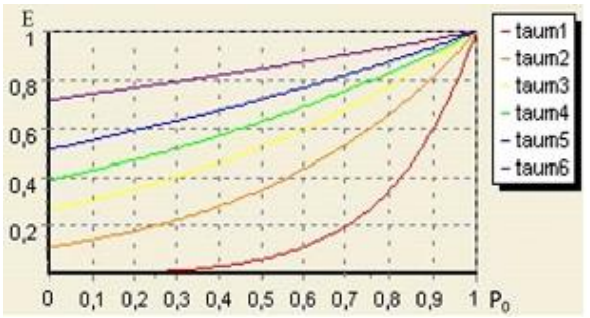
The mathematical models of evaluation criteria for the quality of service operation of CA are developed. Allowable value of static criteria means that it is monitored for integrity only that and even then, when it is provided by the operational documentation for ADPS.

For the estimation of dynamic criteria semi-Markov model are proposed generated for normal ADPS based on the original E-network, and for the reference ADPS - original RMSAS network. These semi-Markov models make it possible to take into account the probabilistic nature of transitions between different states, and the arbitrariness of the laws of distribution of time of transitions at the assumption of independence probability and time transition from the previous transitions.

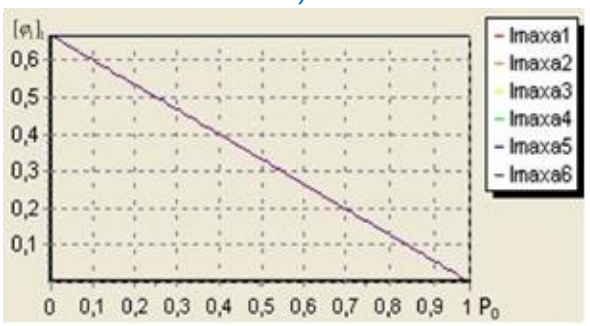
In the DELPHI programming environment we created a complex of problem-oriented software for modeling service management of CA of information processed as in conventional so in reference ADPS. It, in particular, allows us to construct graphic dependences of dynamic criteria, regardless of the variable 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 (see Figure 1).

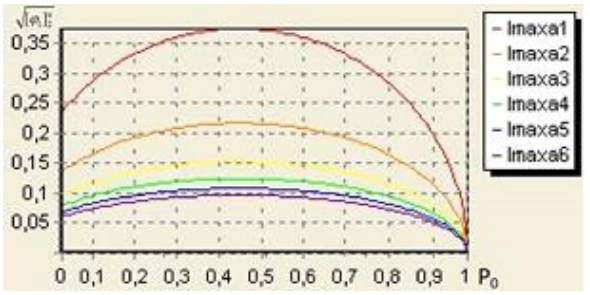
For the reference ADPS the results of calculations were presented in the form of dependencies of output variables from the single (unique for each method), regardless of the varied managed parameter by different $\tau_m = 0{,}1;0{,}3;0{,}5;0{,}7;1;2$ (curves *taum*$_i$, $i = \overline{1,6}$) and a different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



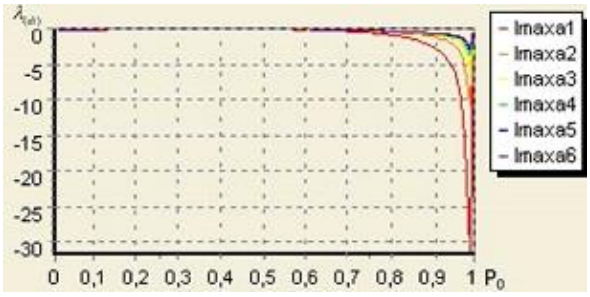
a)



b)



c)



d)

a – criteria of dynamic efficiency;
b – mathematical expectation;
c – standard deviation; *d* – Pearson ratio

Fig. 1 The results of the calculations for the reference ADPS

The output variables are the criteria *E* and the characteristics of the random variable duration of CA in discretionary access:

$[\varphi_1]_k$, $[\varphi_1]_k^u$ – initial and central moments of order $k = \overline{1,4}$; γ_a, $\gamma_э$ – asymmetry coefficient and kurtosis; $A_{(di)}$, $a_{0(di)}$, $b_{0(di)}$, $b_{1(di)}$, $b_{2(di)}$, $D_{(di)}$, $\lambda_{(di)}$ – auxiliary and the first 4 parameters determinant of the quadratic trinomial and characterizing its relationship to the approximating Pearson distribution.

Analysis of the results of calculations, part of which is shown in Figure 1, allows you to identify patterns of governance. They do not contradict the known data and show the opportunities of modeling.

The procedures and the algorithms for optimal control of CA service separately for a typical SIP UA and the reference ADPS by estimated quality criteria for its operation, allowing us to find a compromise between ensuring the integrity and the efficiency of information processing are developed. To estimate the current values of the input variables in the evaluation criteria is intended the quality control subsystem of CA service operation. The calculations are performed by well-known formulas of mathematical statistics processing provided by recording and reporting subsystem of statistical data. According to the results of optimization of controlled parameters is generated a control action by throw-in sensor uniformly distributed on the interval [0, 1] random numbers, making forecast difficult to the attacker. Thus, depending on the return sensor values, the values of the parameters of the next launch of the CA service are generated. For the reference ADPS they are determined like which part of controlled information will be checked for immutability, and in case of IP protection of typical SIP UA is only determined whether to launch service of CA or not.

The results of the application of models of invulnerable circulation of information technology to the standard database managed by the reference object-DBMS, evidence of wide abilities of these models to ensure the availability and confidentiality of information processed in prospective ADPS CA.

4 CONCLUSIONS

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.

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.

The mathematical models of synthesis of policy safe interaction of IP, allowing SP to consider separately the various structural components of RMSAS network with the ability to its further interlinkages have been developed. In particular, the mathematical models of SP in the reference DBMS. Considering as a promising SP DBMS object-relational DBMS, a method of aggregation of its models, providing compatibility with RMSAS are developed.

Using the apparatus RMSAS networks and E-nets 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 in the management of the service of CA are offered.

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. 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.

WORKS CITED

Ahmad, D., Dubrovskiy, A. & Flinn X. (2005). *Defense from the hackers of corporate networks*. Moscow. Companies AyTi; DMK - Press.

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, p. 10.

Chi, S., Park, J., Jung, K. & Lee, J. (2001). Network Security Modeling and Cyber At-tack Simulation Methodology//LNCS. Vol. 2119.

Goldman, R. (2002). A Stochastic Model for Intrusions // LNCS. Vol. 2516.

Gorodetski, V. & Kotenko, I. (2002). Attacks against Computer Network: Formal Grammar-based Framework and Simulation Tool. RAID 2000 // LNCS. Vol. 2516.

Harel, D. (1987). Visual Formalism for Complex Systems, Science of Computer Programming 8. p. 231-274.

Lahno V. & Petrov A. (2010) . Modelling of discrete recognition and information vulnerability search procedures. TEKA. Volume XI A. p. 137-144.

Lahno V. & Petrov A. (2011). Ensuring security of automated information systems, transportation companies with the intensification of traffic. Lugansk. VNU.

Shun-Chieh, L., & Shian-Shyong, T. (2004). Constructing detection knowledge for DDoS intrusion tolerance // Expert Systems with Applications. - 2004. - V. 27. P. 379–390.

Smirniy, M. & Lahno, V. (2009). The research of the conflict request threads in the data protection systems. Proceedings of Lugansk branch of the International Academy of Informatization. V 2(20). p. 23-30.

Received for publication: 16.11.2013
Revision received: 20.12.2013
Accepted for publication: 01.12.2013

How to cite this article?

Style – **APA** *Sixth Edition*:

Lahno, V. (2014, 01 2014). Ensuring of information processes' reliability and security in critical application data processing systems. (Z. Čekerevac, Ed.) *MEST Journal, 2*(1), 71-79. doi:10.12709/mest.02.02.01.07

Stile – **Chicago** *Fifteenth Edition*

Lahno, Valery. "Ensuring of information processes' reliability and security in critical application data processing systems." Edited by Zoran Čekerevac. *MEST Journal* (MESTE) 2, no. 1 (01 2014): 71-79.

Style – **GOST** *Name Sort:*

Lahno Valery Ensuring of information processes' reliability and security in critical application data processing systems [Journal] = Information processes' reliability and security // MEST Journal / ed. Čekerevac Zoran. - Belgrade : MESTE, 01 2014, 2014. - 1 : Vol. 2. - pp. 71-79. - ISSN 2334-7058 (Online); ISSN 2334-7171.

Style – **Harvard** *Anglia:*

Lahno, V., 2014. Ensuring of information processes' reliability and security in critical application data processing systems. *MEST Journal,* 2014 01, 2(1), pp. 71-79.

Style – **ISO 690** *Numerical Reference:*

Ensuring of information processes' reliability and security in critical application data processing systems. **Lahno, Valery.** [ed.] Zoran Čekerevac. 1, Belgrade : MESTE, 01 2014, 2014, MEST Journal, Vol. 2, pp. 71-79. ISSN 2334-7058 (Online); ISSN 2334-7171.