MEST Journal
DOI 10.12709/mest.02.02.02.11

# PROTECTION OF INFORMATION IN CRITICAL APPLICATION DATA PROCESSING SYSTEMS

**Valery Lahno**
Lugansk National Agrarian University, Lugansk, Ukraine


JEL category: **G14, L15, L86**

***Abstract***

*The results of researches, allowing raising the level of protection of the automated data processing systems of critical applications 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 to provide a highly reliable information processing has been developed. The mathematical models of synthesis of policy safe interaction of information processes, allowing security policy 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, the data processing system, security policy, mathematical models*

## 1. INTRODUCTION

Every day, we put our personal information at risk. Whether we're signing up for a newsletter online, or making a transfer at a bank, these activities all involve the transmission of information that could be a problem if it fell into the wrong hands. That's what digital security is so important – it's vital to most of our everyday transactions. New methods are found every day to breach security, and new methods are constantly being developed. There are various ways to authenticate, encrypt, and otherwise protect important information being handled by organizations, and new ones are being added all the time.

In recent years, Intrusion Prevention System (IPS) has been widely implemented to prevent suspicious threats. Unlike the traditional Intrusion Detection System, IPS has additional features to secure the computer network system. IPS is an access control device with a prevention function,

Address of the corresponding author:
**Valery Lahno**
lva964@gmail.com

which enforces a network security policy, is a helpful device that allows for more granular blocking action.

In the last few years, the Internet has experienced explosive growth. Along with the widespread evolution of newly emerging services, the quantity and impact of attacks have been continuously increasing as well. IPS has become an essential component of computer security to predict and prevent attacks. They monitor, identify and recognize all real-time packets inbound and outbound. IPS, which proactively combines the firewall technique with that of the Intrusion Detection System, prevents attacks from entering the network by examining various data records and the detection demeanor of the pattern recognition sensor, when an attack is identified, intrusion prevention blocks and logs the offending data (Ahmad D., Dubrovskiy A. & Flinn X., 2005).

The signature is the primary means to identify activity in network traffic, and the host performs the detection of inbound and outbound packets and to block that activity before damage and network resources are accessed. However, IPS can effectively detect suspicious threats that are already known from a list of signatures. Common Vulnerability Exposure (According - cve.mitre.org) is a list of intruding products, and there are several IPS devices with proprietary standards. For this reason, many IPS vendors dedicate a large number of engineers to continuous observation of suspicious threats and update their product database with new signatures as threats arise (Shun-Chieh Lin & Shian-Shyong Tseng, 2004).

## 2. PREVIOUS RESEARCHES

Information security management has become a critical and challenging business function because of reasons such as rising cost of security breaches, increasing scale, scope and sophistication of information security attacks, complexity of information technology (IT) environments, shortage of qualified security professionals, diverse security solutions from vendors, and compliance and regulatory obligations (Goldman R., 2002).

The introduction of information technologies includes an associated level of risk, but specific security features can be incorporated into a system to mitigate that risk (Chertov R., Fahmy S., & Shroff N., 2006).

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. 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.

The reason lies in the fundamental theoretical difficulties of modeling technologies ensuring the reliability and protection of information processes (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 S., Park J., Jung K. & Lee J., 2001).

Any model of the security policy (SP) to ensure the highly reliable information processing (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 (Gorodetski V. & Kotenko I., 2002).

The object of the study, the results of which are presented in this article are HRIP processes with

flexible protective mechanisms. The subject 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 (Harel D., 1987).

A method of hierarchical structuring of IP resources in ADPS, providing unity consider global and local SP reference model of secure automated system (RMSAS) has been provided. A fifteen-layer RMSAS structuring as an extension of the well-known seven-layer OSI model in the direction of decomposition of its application layer has been proposed (see Figure 1).

Leveled of security systems services (SSS) includes leveled object control (OC), service CA, security monitor (SM), consisting of a security monitor objects (SMO) and the safety monitor subjects (SMS).

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.

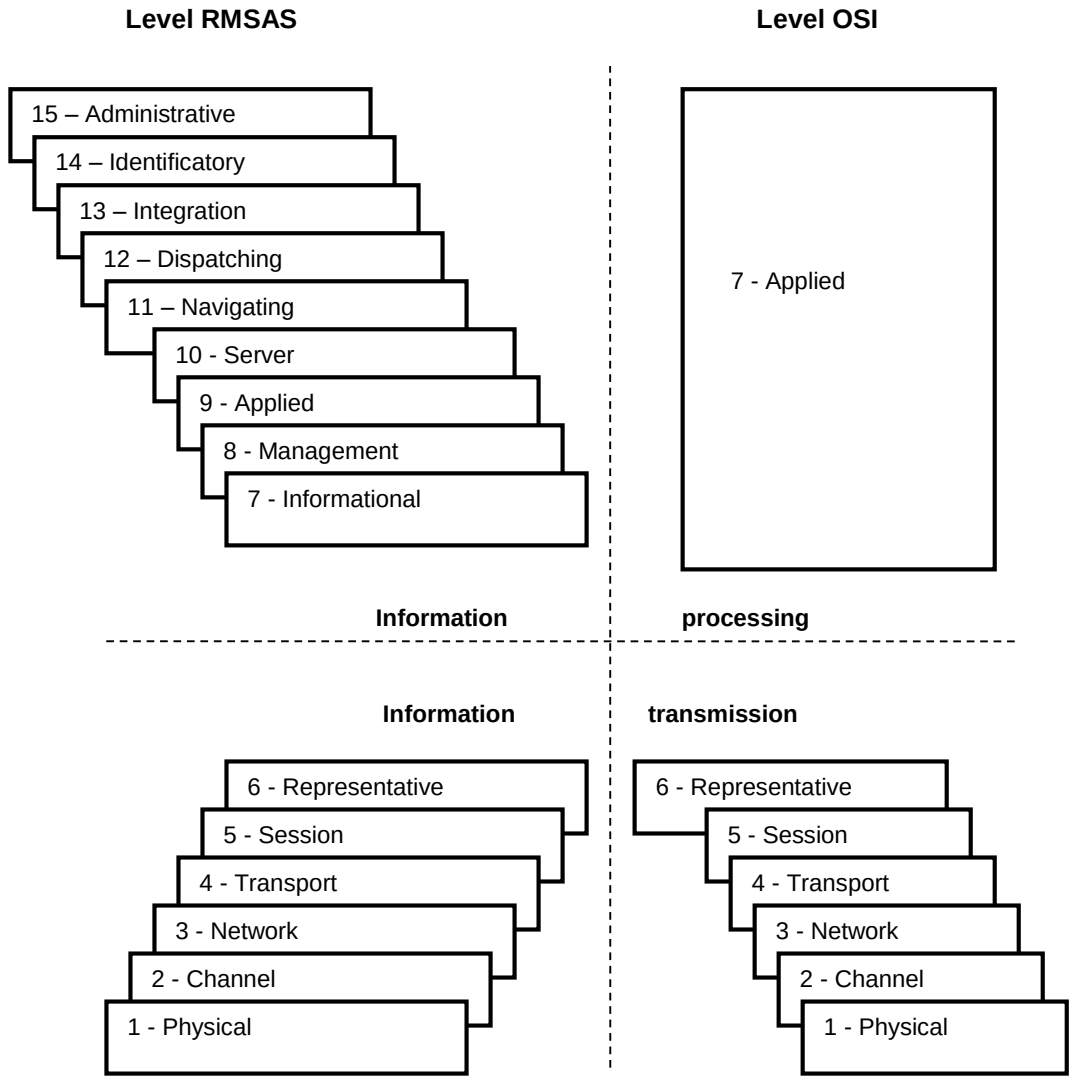



*Fig. 1. The hierarchical structuring of IP resources in ADPS*
*Source: Rogozin E., 2003*

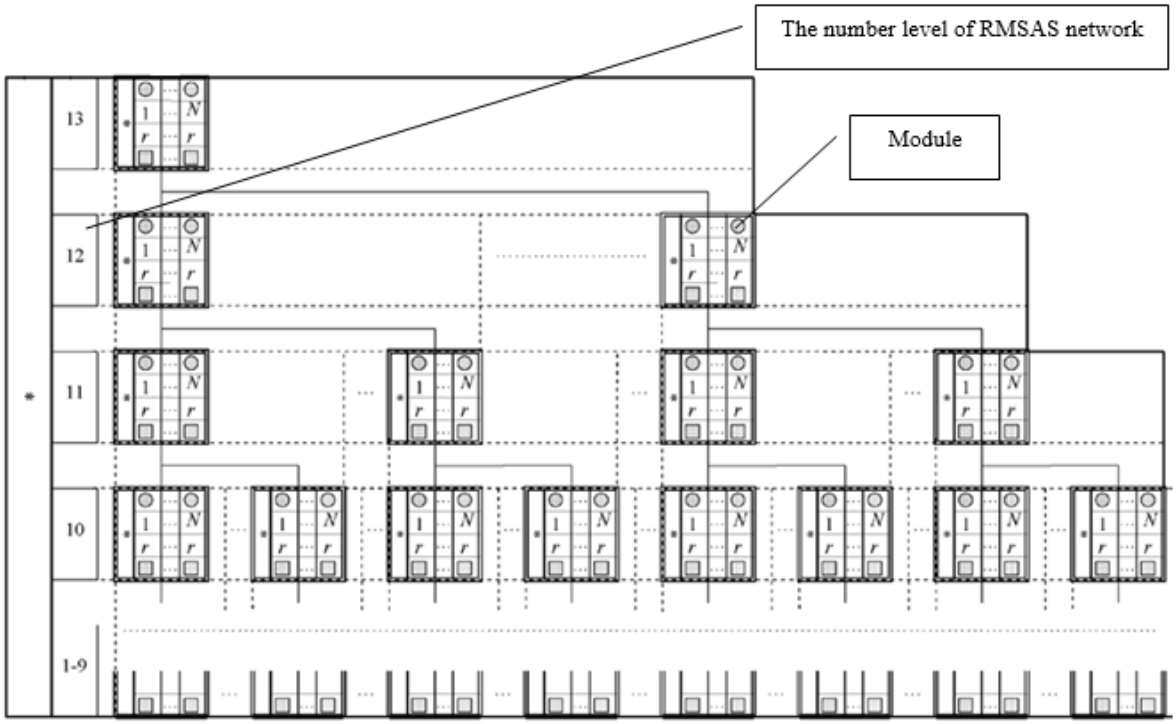



*Fig. 2. Graphical representation of the reference model of the protected automation system (network) in the canonical form (Source: (Goldman R., 2002))*

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 (Rogozin E., 2003).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 (see Figure 2).

## 3. THE FUNDAMENTAL THEOREM OF SECURITY FOR DISCRETIONARY SECURITY POLICY FOR SUPERBLOCK RMSAS NETWORK

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 $B_0 = S_{1..L}$ is *(in the network interpretation)* part of RMSAS network related to the levels of RMSAS with numbers $l = \overline{l_H, l_в}$.

Superblock $S_{l_H \ldots l_в}(I)$ of the level $l_H$ with the index $I$ (given superblock of RMSAS network $S_{l_H \ldots l_в}$) of RMSAS network $B_0 = B_{1..L}(0)$ 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 $\Psi_1$ and $\Psi_2$, denoted as $\Psi_1 \sim \Psi_2$ is the lack of direct conflict between them. Strong compatibility of random SP $\Psi_1$ and $\Psi_2$, denoted as $\Psi_1 \approx \Psi_2$ is the inability of a conflict between them, even in distributing of SP to all RMSAS network.

Layerwise synthesis of security policies of RMSAS network is a synthesis of the SP of RMSAS network in general suitably chosen its ultimately degraded by multiple superblocks. Methods of such expansions are defined by specifying RMSAS network of relevant half rings quantities. In particular, when using a layerwise synthesis of SP on superblocks of database management system (DBMS) (formalized to access information directly in RMSAS) used half ring

$$\left\{ \begin{matrix} \varnothing; \mathrm{B}_0; B_{10...13}(0); \\ B_{7...9}(I(u)) \end{matrix} \middle| \begin{matrix} u \in U_9; \\ B_{1...6}(I(u)) \end{matrix} \middle| u \in U_6 \right\} \quad (1)$$

layered superblock structure of RMSAS network, given of its partition into adjacent layers $\{S_{1...6}, S_{7..9}, S_{10...13}\}$, or half ring

$$\left\{ \begin{matrix} \varnothing; \mathrm{B}_0; B_{9...13}(0); \\ B_{7...9}(I(u)) \\ B_{1...7}(I(u)) \end{matrix} \middle| \begin{matrix} u \in U_9; \\ \\ u \in U_7 \end{matrix} \right\} \quad (2)$$

layered superblock structure of RMSAS network, given of its covering of the related layers $\{S_{1...6}, S_{7...9}, S_{10...13}\}$.

For the analysis of aspects of security of information processed in the reference ADPS (integrity, availability and confidentiality of information) are developed their mathematical model. At the same time, confidentiality and availability of modeling is carried out through the research of the mathematical properties of the SP complex of RMSAS network and the integrity of the modeling – through the modeling of optimal CA control service of information processed in the reference ADPS (Lahno V. & Petrov A., 2010).

Ensuring the confidentiality is modeled as a range of SP for RMSAS network as a whole or as a particular superblock. Given a super-block *B* with the quantities $P_H(B)$, $P_l(B)$ and $P(B)$ allowing the lower positions of *l*-th and all other levels quantities $U_l(B)$ and $U(B)$ of modules *l*-th and all other levels, in this SP superblock complex.

Then execution on superblock *B* of the global SP $\Psi_g(B)$, discretionary *l*-th level of SP $\Psi_{\partial l}(B)$, SP-leveled local $\Psi_{ll}(B)$, local SP $\Psi_l(B)$ and discretionary SP with permits respectively $\Psi_{\partial p}(B)$ means:

$$(\forall p = p[I,\alpha] \in P_H(B) \setminus \Psi_g(B))(M_{out}[I,\alpha] = 0); \quad (3)$$

$$(\forall p = P[I,\alpha] \in P_l(B) \setminus \Psi_{\partial l}(B))(M_{out}[I,\alpha] = 0); \quad (4)$$

$$(\forall p = p[I(u),\alpha] \in P_l(B) | u \in U_l(B), \alpha = \overline{1,N}, \langle I(u),\alpha,0\rangle \in \Psi_{ll}(B)); \quad (5)$$

$$(M_{out}[I,\alpha] = 0)$$

$$(\forall p = p[I(u),\alpha] \in P(B) | u \in U(B), \alpha = \overline{1,N}, \langle I(u),\alpha,0\rangle \in \Psi_l(B)); \quad (6)$$

$$(M_{out}[I,\alpha] = 0)$$

$$(\forall p = p[I,\alpha] \in P(B) \setminus \Psi_{\partial p}(B)) \cdot (M_{out}[I,\alpha] = 0). \quad (7)$$

Development of the model of information confidentiality allowed a rigorous mathematical modeling at the SP level to prove in the following theorems the invulnerability of information in the reference ADPS on the aspect of confidentiality, that means that for any given access discretionary authorities to the physical or arbitrary level of RMSAS is determined by its supporting rules of safe intersubjective control, performing that unauthorized access impossible.

*The fundamental theorem of security for discretionary SP for superblock RMSAS network.* If at the initial moment given discretionary SP is performed at a certain superblock, and all the movements of chips satisfy the inducing local SP on the same superblock, then at any time thereafter, this given discretionary SP on superblock is also performed.

*The fundamental theorem of security for the global SP superblock RMSAS network.* If at the initial moment is performed inducing given global SP at a certain superblock discretionary SP in the same superblock, and all the movements of chips satisfy a given the inducing global SP of local SP at this superblock, then at any time thereafter, will be performed given global SP at this superblock.

Ensuring of information accessibility is modeled as a attainability of labeling induced by this SP of RMSAS network in general or on a particular superblock of the root labeling.

*Root labeling of RMSAS network* is characterized by all common positions contain the top-level chip, but none of other positions of RMSAS network does not contain a chip, which is interpreted as the absence of hyperprocesses in the reference ADPS:

$$\begin{aligned}&(\forall p = p[I,\alpha] \in P_L)(M_{in}[I,\alpha] = 1 \wedge \\ &\wedge M_{out}[I,\alpha] = 0) \wedge \\ &\wedge (\forall p = p[I,\alpha] \in P \setminus P_L) \cdot \\ &(M_{in}[I,\alpha] = M_{out}[I,\alpha] = 0).\end{aligned} \quad (8)$$

Labelling of RMSAS network induced by a given discretionary SP with globalized performance $\Omega_{\partial z}$, characterized by the fact that all positions of a globalized quantity of allowed positions of the discretionary SP contain a chip, but none of the other entries of RMSAS network does not contain a chip, which is interpreted as the implementation of discretionary access to the resources of the reference ADPS to the maximum authority stipulated for given discretionary SP:

$$\begin{aligned}&(\forall p = p[I,\alpha] \in \Psi_{\partial z})(M_{in}[I,\alpha] = 0 \wedge \\ &\wedge M_{out}[I,\alpha] = 1) \wedge \\ &\wedge (\forall p = p[I,\alpha] \in P \setminus \Psi_{\partial z}) \cdot \\ &(M_{in}[I,\alpha] = M_{out}[I,\alpha] = 0).\end{aligned} \quad (9)$$

Labelling of RMSAS network induced by the given global SP is defined as induced discretionary SP, inducing given global SP.

Development of the model of availability of information mathematically rigorous allowed at the level of SP models to prove the following theorems of invulnerability of information processed in the reference ADPS, on aspect of the availability, which means that for any given discretionary powers of access to the physical or arbitrary level of RMSAS are uniquely determined their supporting rules of safe management of intersubject under which the legal access is possible.

*The fundamental theorem of attainability for discretionary SP superblock of RMSAS network:* For any given discretionary SP at this superblock is always possible to determine the permitting processes and procedures of the conversion for all the modules of the superblock that induced this discretionary SP at this superblock its labeling less attainable from its root within labeling of the inducing this discretionary SP by local SP at this superblock.

*The fundamental theorem of for the global attainability SP on superblock of RMSAS network:* For any given global SP at this superblock is always possible to determine the permitting processes and procedures of for the conversion all the modules of the superblock that induced this global SP at this superblock its labeling less attainable from its root labeling of within the inducing this global SP by local SP at this superblock.

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 (see Figure 2). 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 case of IP protection of typical SIP UA models of estimation of two dynamic criteria are represented respectively by two finite semi-Markov processes (FSP) with different initial and final states. In the case of the reference ADPS, two dynamic criteria expressed in terms of an auxiliary *criteria of dynamic efficiency E*, the model for the evaluation of which is represented by its FSP. Each FSP is described by its semi-Markov matrix $H(\tau) = \|H_{ij}(\tau)\|$, $i = \overline{1,n}$, $j = \overline{1,n}$, formed based on the original network. Its element is $H_{ij}(\tau) = p_{ij}G_{ij}(\tau)$, where $p_{ij}$, $G_{ij}(\tau)$ – are probability and probability distribution function of FSP transition time in a state *i*, directly to the state *j*.

Each of the criteria $E_{af}$, $E_{ta}$ (in case of IP protection of typical SIP), *E* (in case of a reference ADPS) is the probability of reaching a timely corresponding FSP absorbing state. In this way, the dynamic criteria are formalized as temporal and probable characteristics (TPC) of service operation of CA information processed in ADPS. The starting basis for the investigation of such TPC and lifetimes of FSP is in general case, the system of TPC dynamics that in original looks like:

$$Q_i(\tau) = H_{in}(\tau) + \sum_{j=1, j\neq i}^{n-1} \int_0^{\tau} H_{ij}(t) \cdot Q_j(\tau - t)dt, i = \overline{1,n-1}; \quad (10)$$

$$\begin{aligned} (I - \overline{H}(v))q(v) &= h(v), \\ (I - \overline{H}(0))\alpha &= h(0) \end{aligned}, \quad (11)$$

where:

*I* – identity matrix;

$\overline{H}(v) = \|h_{ij}(v)\|$,

$i = \overline{1,n-1}$,

$j = \overline{1,n-1}$;

$h(v) = (h_{in}(v))$,

$q(v) = (q_i(v))$,

$\alpha = q(0) = (\alpha_i)$,

$i = \overline{1,n-1}$;

$h_{ij}(v)$, $i = \overline{1,n-1}$, $j = \overline{1,n}$ – Laplace-Stieltjes transformation of function $H_{ij}(\tau)$;

$\alpha_i$, $Q_i(\tau)$ – the probability of absorption FSP in state *i* at any time and less than $\tau$, $q_i(v)$ – Laplace-Stieltjes transformation of function $Q_i(\tau)$.

Dependences (10) and (11) are obtained using semi-Markov matrix formalism for integrating the matrix formalism of finite Markov chains and operator formalism of random processes in a single review of continuous-time and discrete states.

The timeliness of the FSP absorption is determined by formulas:

$$\alpha = (I - \overline{H}(0))^{-1}h(0);$$
$$v_m = 1/\tau_m;$$
$$q(v_m) = (I - \overline{H}(v_m))^{-1}h(v_m);$$
$$E = q_1(v_m),$$

where $\tau_m$ – the average value of the exponential probability distribution of the FSP maximum lifetime.

There were also found the formulas for calculating the number of characteristics of the FSP lifetime. The proposed accurate analytical method requires small amounts of computation with no restrictions on the structure of the formalized network. Therefore, these models are more efficient than analytical and imitational, traditionally used in reliability theory of IP and other technical applications researching TPC systems.

The task of a making decision is formalized as a task of mathematical programming. You must select an alternative $a \in A$ from a quantity of alternatives *A* so, as to satisfy:

$$E_{af}(a) \to \max; \quad (12)$$

$$E_{ta}(a) \geq E_{\min ta}; \quad (13)$$

$$E_{fa}(a) \wedge E_{ra}(a) \wedge E_{fa}(a) \wedge E_{yu}(a) = 1, \quad (14)$$

where:

$E_{minta}$ – defined according to the ADPS operational documentation constant;

*a* – alternative characterized by controlled service operation parameters of CA.

In the case of IP protection of typical SIP UA is used unique controlled parameter $P_{kc}$ – the probability of launch of the service of CA in the next work session. For the reference ADPS managed parameters are multiple with different ways of their variation.

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 (Smirniy M. & Lahno V., 2009).

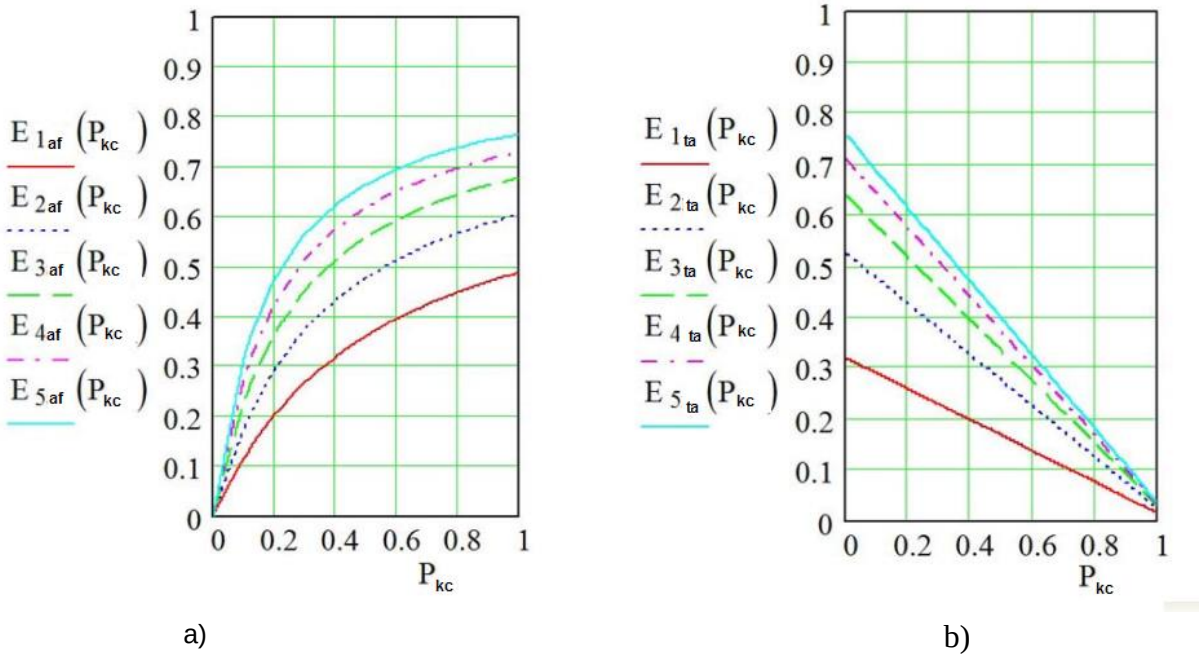
In order to strengthen the protection of information resources the enterprise managers are invited to use a continuous adjustment of profiles of active users, in particular, the so-called iterative algorithm (IA). The meaning of the iterative algorithm is in implicit feedback of server with a user, implemented through the request statistics registration. The obtained evaluation of the current user profile is used to rank the users into groups according to the degree of danger for IP resources: a) user, b) potentially dangerous user, c) dangerous user, d) the offender. For the synthesis of the automatic classification a discrete procedures unit of recognition of threats and vulnerability, described in detail in works (Lahno V. & Petrov A., 2010-2011), is applied.

## 4. THE SIMULATION RESULTS OF THE ADPS

With the help of the developed software conducted a comprehensive study on the quality of functioning of a typical system to security information from unauthorized access by the example of "Spectrum-X», in relation to the operation of workstation-based computer into an automated data processing system (Figure 3).

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.

Therefore, the construction and the research of these relationships represents a significant interest to the theoretical research of the patterns of CA service management, see Fig. 3.




a) b)

a) Dependence of the criterion $E_{af}$ controlled parameter $P_{kc}$;
b) Dependence of the criterion $E_{ta}$ controlled parameter $P_{kc}$

*Fig. 3. Results of calculations for a typical system of information security "Spectrum-X"*

For a typical system of information protection (for example, *"Spectrum-X"*), the results of calculations presented in the form of dependency $\mathrm{E}_{\mathrm{iaf}}(P_{kc})$ and $\mathrm{E}_{\mathrm{ita}}(P_{kc})$, $i=\overline{1,5}$ criterion $\mathrm{E}_{\mathrm{af}}$ and the criterion $\mathrm{E}_{\mathrm{ta}}$ of the controlled parameter for different values of the other variable parameters. In Figure 3, the curves $\mathrm{E}_{\mathrm{iaf}}(P_{kc})$, $\mathrm{E}_{\mathrm{ita}}(P_{kc})$ different values of $\tau_{\mathrm{maf}}=3600\cdot(i+1)$ and $\tau_{\mathrm{mta}}=60\cdot i$, respectively, where $\tau_{\mathrm{maf}}$, $\tau_{\mathrm{mta}}$ are the averages the maximum time between adjacent integrity checks and implementation of the system of protection of its functions. Any increase depending interpreted as an improvement (by this criterion) quality of service IC as a control object with the growth of the controlled parameter and decrease - as deteriorating.

## 5. CONCLUSIONS

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.

After completion of the entire previously mentioned stages one can start the work on forming the model of information threats for all the information resources of the enterprise on the

basis of the derived classifiers. The initial data for simulation are classes of vulnerabilities, threats and attacks, and also multitudes of RMSAS attack realization means and categories (classes) of malefactors.

The problem of using proper characteristic functions was not considered in corpore within the bounds of this research, as there are different mathematical approaches to descriptions of characteristic functions, which can be found for each class of information attack targets. For example, the following methods are used for solving problems connected with simulating the speed of malicious software spreading, that is measuring the percentage of infected computers within the network:

1) models based on changed systems of differential equation, formulated in classic epidemiologic models;
2) models based on calculation of Hamiltonian path length in the part of the analogous graph, where spreading is still possible;
3) other.

## 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.

Rogozin E. A. E- network presentation of functioning of the perspective programmatic system of priv. Journal - Questions of information security. - 2003. N 3(62). - P. 71-74.

Shun-Chieh Lin & Shian-Shyong Tseng. (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: 08.01.2014
Revision received: 29.03.2014
Accepted for publication: 27.04.2014

***How to cite this article?***

*Style – **APA** Sixth Edition*

Lahno, V. (2014, 07 15). Protection of information in critical application data processing systems. (Z. Čekerevac, Ed.) *MEST Journal, 2*(2), 102-112. doi:10.12709/mest.02.02.02.11

*Style – **Chicago** Fifteenth Edition:*

Lahno, Valery. 2014. "Protection of information in critical application data processing systems." Edited by Zoran Čekerevac. *MEST Journal* (MESTE) 2 (2): 102-112. doi:10.12709/mest.02.02.02.11.

*Style – **GOST** Name Sort:*
**Lahno Valery** Protection of information in critical application data processing systems [Journal] // MEST Journal / ed. Čekerevac Zoran. - Belgrade : MESTE, 07 15, 2014. - 2 : Vol. 2. - pp. 102-112.

*Style – **Harvard** Anglia:*
Lahno, V., 2014. Protection of information in critical application data processing systems. *MEST Journal,* 15 07, 2(2), pp. 102-112.

Style – **ISO 690** Numerical Reference:
*Protection of information in critical application data processing systems.* **Lahno, Valery.** [ed.] Zoran Čekerevac. 2, Belgrade : MESTE, 07 15, 2014, MEST Journal, Vol. 2, pp. 102-112.