computing@tanet.edu.te.ua
www.tanet.edu.te.ua/computing

ISSN 1727-6209
International Scientific
Journal of Computing

INTEGRATED SYSTEMS OF INFORMATION SECURITY IN COMPUTER NETWORKS

Georgy Loutsky, Valerij Shyrotchin, Vadim Mukhin

National Technical University of Ukraine "Kiev Polytechnic Institute"
Ukraine, Kiev, Pr. Pobedy, 37
E-mail: mukhin@comsys.ntu-kpi.kiev.ua

Abstract: *In this paper we suggest the integrated security systems for computer networks, which are adaptive to certain network parameters. Also is suggested the approach to adaptive security systems parameters evaluation based on the analysis of information value changing in time. The main requirements to adaptive security systems are developed.*

Keywords: *Integrated security systems, adaptation, parameters evaluation, information value.*

1. INTRODUCTION

The modern computer networks are dynamically changing objects. The number of network units and servers are varied frequently, and also various network applications are running there. These facts cause the necessity in development of the new approaches and mechanisms for the information security in the computer networks. Any modification in software/ hardware resources results in changing of the accepted safety policy in computer system, in arising of the backdoors in security mechanisms and the new ways for information leakage. [1,2]

The security department, which installed the security mechanisms and are monitoring the computer system operations, should perform the adaptation of these mechanisms to new network parameters and new resources usage. The creation of the special supporting tools for security mechanisms adaptation to the required safety policy in computer systems and networks is rather actual scientific and technical problem. [3,4]

2. METHODS AND MECHANISMS FOR THE DATA SECURITY IN THE COMPUTER SYSTEMS AND NETWORKS

There are several approaches to the development and to the implementation of the security mechanisms in computer systems and networks. A methodological basis for their development is the standards of the International Organization on Standardization (ISO) and the standard models for interaction in the open systems. [5,6]

In general, there are three main approaches to the secured computer systems and networks design: [2]

1) development of the new secured computer systems, in which all security mechanisms are implemented during creation (the creative approach).

2) updating the existing computer systems with new security mechanisms (the additive approach).

3) development of the security mechanisms and modules, that realizes the functions of data safety insurance, and their adaptation to the security mechanisms that are already used in the computer systems and networks (the adaptive approach).

The adaptive approach eliminates some shortcoming of the two other approaches, and inherits the advantages of the additive (the compatibility with standard software), and the creative approaches. Fig 1. shows the generalized model of computer systems with the adaptive security mechanisms.

The subjects of a computer system (users, active processes, etc.) can get access to the objects (passive information resources) only under the control of the adaptive safety monitor, that performs filtration of the data flow, and transfers the data flow of the legal subjects only. This monitor uses the access rules database to define if certain subject has rights to get access to certain object, and generates the audit records, which contain the data on all the subjects' actions in the computer system.

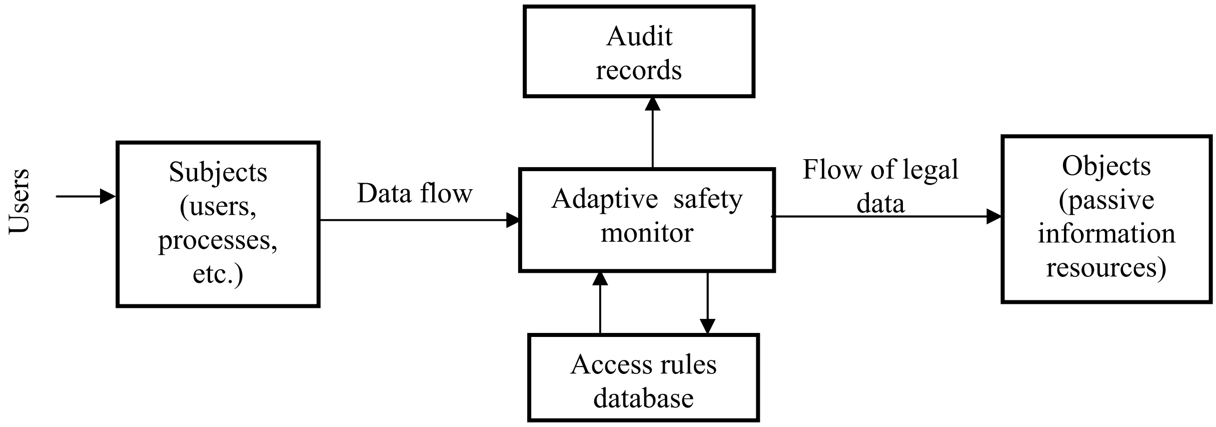


Fig. 1. Model of computer systems with the adaptive security mechanisms

The adaptive safety monitor may change some access rules in the database in the on-line mode due to the current parameters of the computer system safety, for example, basing on the analysis of the audit records of the subjects' actions.

So, the adaptive security systems support adjusting and control features for the software-hardware security means, perform their periodical auditing and overall safety policy evaluation after any system reconfiguration, updating or ISO standards changing.

3. METHODS FOR THE ADAPTATION OF SECURITY MECHANISMS IN COMPUTER SYSTEMS AND NETWORKS

The design of the adaptive security mechanisms is a complex process. We suggest perform this design by following the stages shown in Fig. 2. The main active persons in this process are: information owners, information systems owners and agents of competitive organizations.

The information owners are the persons, who have some data that need to be protected from the unauthorized access. The information systems owners are the persons who give their computer systems to manipulate the data of the information owners. In particular cases, the information owners and the information systems owners may be the same persons. The agents of competitive organizations are the persons who try to get the unauthorized access to the protected data of the information owners.

The stages of the adaptive security mechanisms' design are as follows. First, the information owners generate the requirements to the information systems owners, which intend to minimize the risks of possible losses of the information. Then the information systems owners generate a decision on the information audit technology and a decision on the new security mechanisms finance support. On the next step, the information systems owners realize the counteractions to the possible attacks and threats, based on the analysis of computer system vulnerabilities due to the threats and modifications and on the analysis of information losses risks due to the threats and modifications. At this stage, the system generates the decisions on the security system modifications, on the safety policy audit, and is performing the new leakage ways analysis. These results are the basis for decision on the security mechanisms adaptation to the required parameters of computer system safety (e.g. security level). The agents of competitive organizations perform their own analysis of the security systems parameters and try to realize the unauthorized access to the protectted information. All their actions are under monitorring, are stored in the audit records, and are one of the sources for new threats and leakage ways analysis. And finally, the realization of all the above mentioned stages allows to design the adaptive security system that will react in on-line mode to possible attacks on the computer system, taking into consideration the dynamics of changing information value.

4. THE PARAMETERS EVALUATION OF THE ADAPTIVE SECURITY SYSTEMS

After the design of adaptive security mechanisms for computer systems is complete, we have to research the main parameters of the designed mechanisms. The most typical parameters during quality research of the adaptive secured systems are uncertain factors with unknown distribution.

The methodical evaluation of the uncertain or fuzzy factors is based on the special criteria for decisions on security mechanisms modification. The criteria of Walde, Savige, Gurwitz and Laplace are widely used in the decisions support theory. [7,8]

According to the Walde criterion, the optimal is the strategy which ensures a result that is not worst than "the lower price of game with a nature". The decision, accepted in this way, is free from risk.

To obtain the conciliatory solution between a pessimistic evaluation by the Walde criterion (*W*) and an optimistic maximax evaluation by Savige (*S*), it is suggested to use Gurwitz criterion (*G*):

$$G = \mu * W + (1 - \mu) * S \qquad (1)$$

where: μ, parameter of pessimism-optimism, is determined by the experts, performing the analysis of security systems parameters.

The parameter μ $(0 < \mu < 1)$ is defined on the analysis of weighted vector, that contains the parameters of the security mechanisms (such as security level, performance, probability of the unauthorized access, price, etc). If expert believes, that the security mechanisms are effective enough, then the μ parameter will be less than 0.5 (may tend to 0), and, otherwise, μ will be more than 0.5 (may tend to 1).

So, we can accept the strategy for security mechanisms modification with the maximal Gurwitz criterion value, that is the compromised decision.

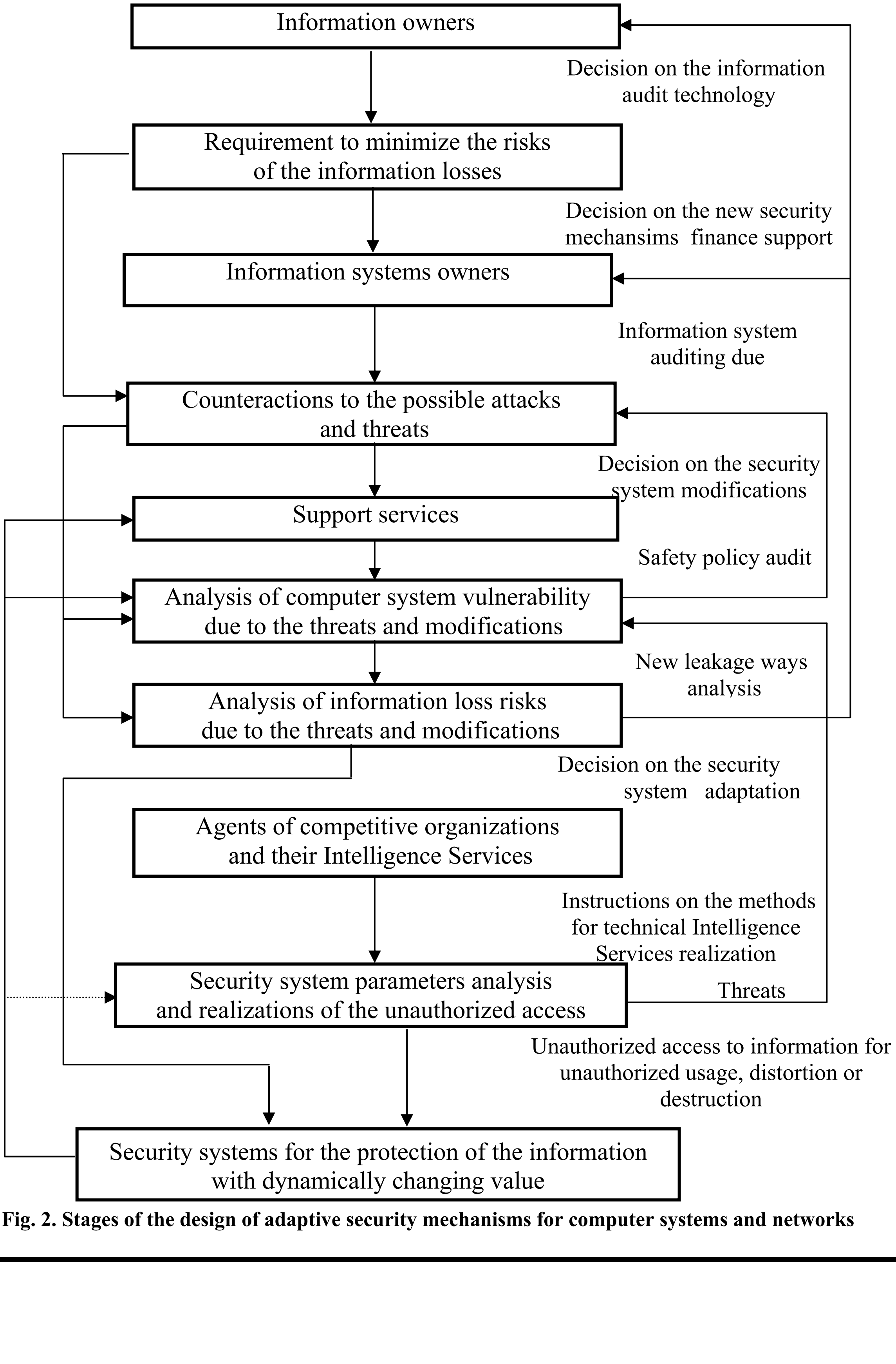

Information owners
Decision on the information audit technology
Requirement to minimize the risks of the information losses
Decision on the new security mechansims finance support
Information systems owners
Information system auditing due
Counteractions to the possible attacks and threats
Decision on the security system modifications
Support services
Safety policy audit
Analysis of computer system vulnerability due to the threats and modifications
New leakage ways analysis
Analysis of information loss risks due to the threats and modifications
Decision on the security system adaptation
Agents of competitive organizations and their Intelligence Services
Instructions on the methods for technical Intelligence Services realization
Security system parameters analysis and realizations of the unauthorized access
Threats
Unauthorized access to information for unauthorized usage, distortion or destruction
Security systems for the protection of the information with dynamically changing value

Fig. 2. Stages of the design of adaptive security mechanisms for computer systems and networks

5. EVALUATION OF THE INFORMATION LOSSES RISKS

One of the important parameters of the adaptive security system is the level of risk for safety threats to the information. The optimal are those security methods and mechanisms that ensure the minimal risk for the threats realization in each certain situation.[9,10]

In the most cases, we protect the information from unauthorized access. In turn, the information value, i.e. the real cost or amount of the losses in case of its destruction or breach of confidentiality, changes according to the information type.

According to the above mentioned parameters, we suggest the information classification depending on its value dynamically changing over time: [11]

1. the information value is constant in time (the information is actual for a long time period, e.g. is stored in a database system);
2. the information value is constantly increasing (the information is accumulating in databases);
3. the information value is constantly decreasing (the information becomes less interesting over time);
4. the information value has top-extremum (the information is related to external events, which may change its status, for example – patent information, information about election campaign, etc);
5. the information value has low-extremum (theoretically possible situation).

The information value (V) means the “material profit” for users, that they can get upon the best usage of the secured information or correspondent losses, which users would have due to the information distortion or destruction. The information value V is calculated as:

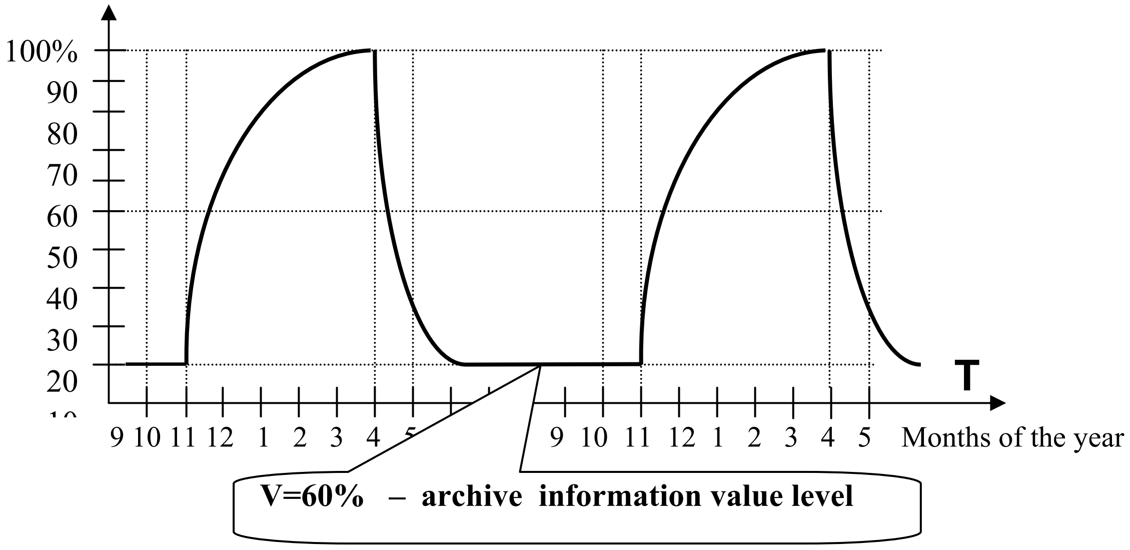
$$V = \sum_{i=1}^{n} w_i * p_i \qquad (2)$$

where p_i – possibility of the unauthorized access in situation i, w_i - possible material loss due to this unauthorized access realization.

On Fig.3-5 are shown the biases, illustrating how may change the value of the economical and tax information. These biases are based on the real data.

Fig 3. shows the changing value of the secured economical and tax information during some research period. This tax information is the data on the persons tax payments. As it shown on Fig.3 there is one tax deadline (for example, in Ukraine on 1 April) per year.

The departments of the State Tax Administration have to collect the maximal volume of the tax data before 1 April and to calculate the payments/ repayments to the state budget, that certain person have to do. After this deadline passes, most (90-95%) tax payments are already transferred, so this information is transformed into archive data. This situation is repeated annually.



V=60% – archive information value level

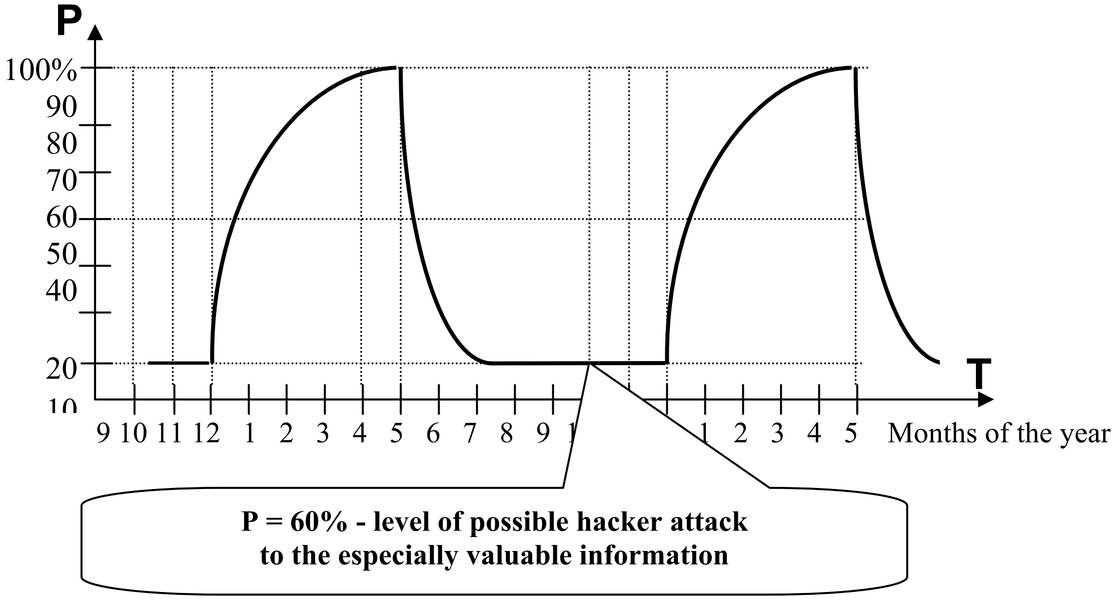
Fig.3. The example of the economical and tax information value changing (in compare to its maximal rate

Fig.4 shows the risk of the same information being distorted or destructed during the researched period. The risk of information distortion or destruction can be very high (near to 100%) in some periods, so we have take it into consideration when designing the security means for computer systems.

Fig.5 shows the dependence between the secured information value and safety administrating charges to support it in the secured state. It is obvious that these administrative charges are increasing along with an increase in information value, but they should be increased in advance, to allow the launch of preventive actions on the information security insurance.

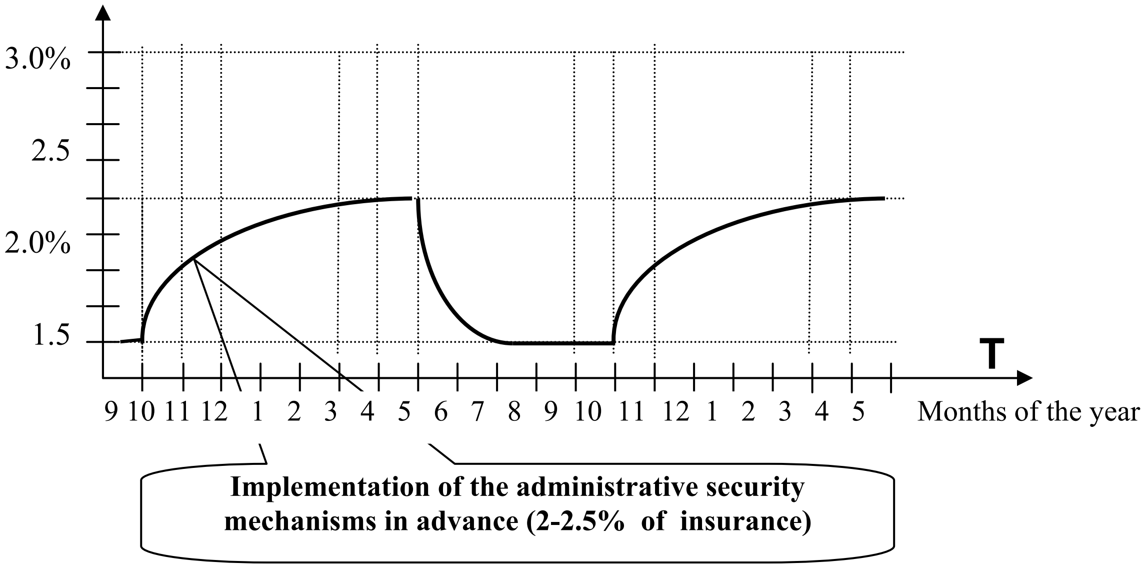
We suggest the following approach to the estimation of computer networks reliability and security level, based on analysis of the safety threats risks and of the changing information value, that is realized in 4 steps:

- find the risks factors and estimate their weights for the dynamics of information value;
- design the general model of computer network, including risks factors influences;
- rate the vulnerable nodes in computer network by their risk level;
- estimate the overall security and reliability level required for the network.



P = 60% - level of possible hacker attack to the especially valuable information

Fig.4. The risk of the information distortion or destruction



Implementation of the administrative security mechanisms in advance (2-2.5% of insurance)

Fig.5. The dependence between the secured information value and safety administrating charges

6. THE MAIN REQUIREMENTS TO THE ADAPTIVE SECURITY SYSTEMS

Based on the above described principles, we formulate the main requirements and specifications for the adaptive security systems. (Fig. 6)

First of all, it is necessary to evaluate the system safety parameters, such as security level, performance, information value, reliability, etc. The main goal of this stage is to define the varying parameters.

The next step is to re-evaluate the system safety goals. This re-evaluation realizes with the safety monitoring mechanisms, which perform the network attacks detection and, in the result, reveal possible threats and information leakage ways in the computer systems.

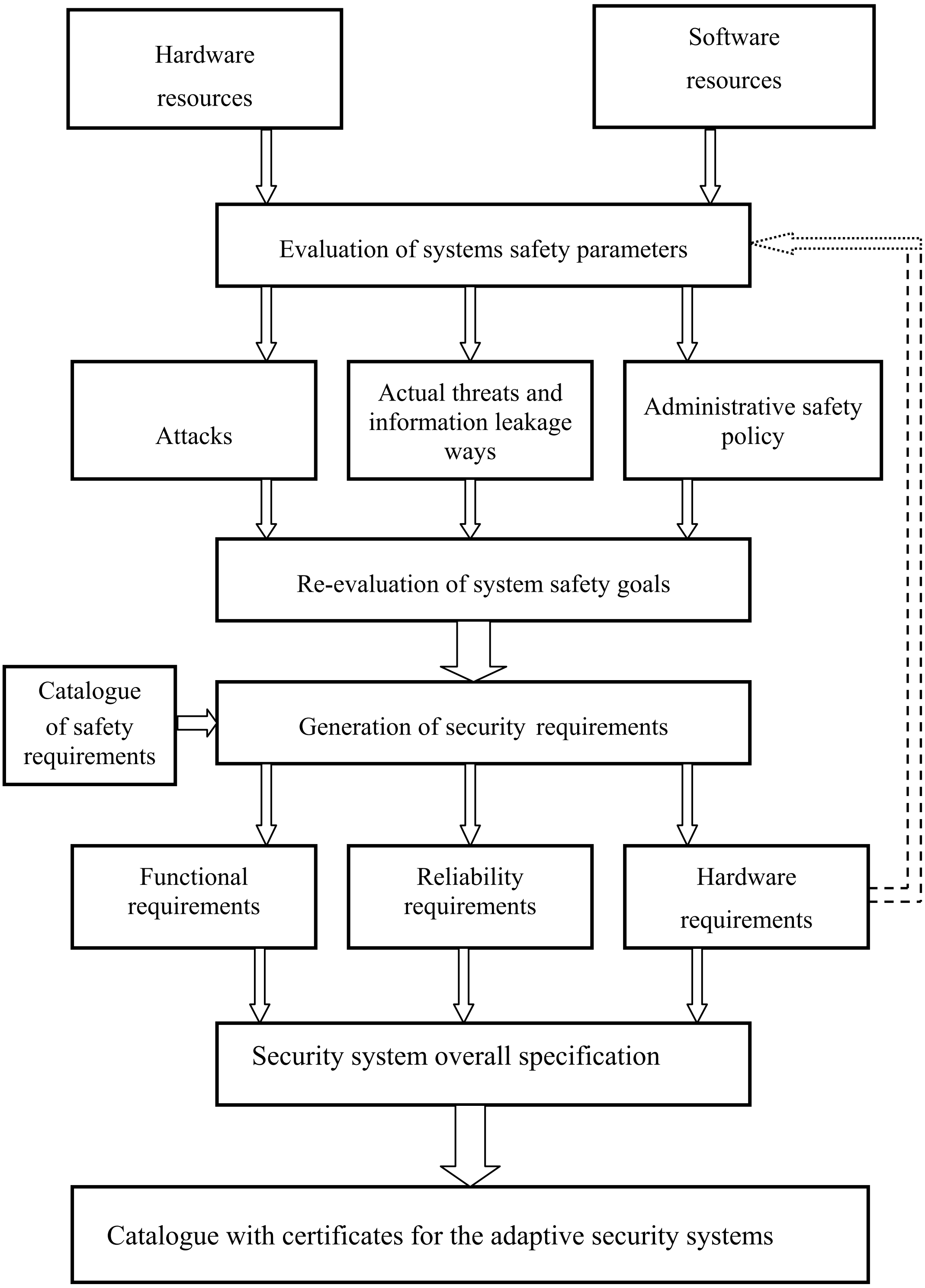

Hardware resources
Software resources
Evaluation of systems safety parameters
Attacks
Actual threats and information leakage ways
Administrative safety policy
Re-evaluation of system safety goals
Catalogue of safety requirements
Generation of security requirements
Functional requirements
Reliability requirements
Hardware requirements
Security system overall specification
Catalogue with certificates for the adaptive security systems

Fig. 6. The main requirements and specifications to the adaptive security systems

The important requirement to the monitoring mechanisms is that they must correctly detect the all poorly secured units in the computer systems. Also on this stage is analyzed the adequacy of administrative safety policy to the required safety level for computer system.

The requirements to security mechanisms are generating on the base of this re-evaluation and on the data from the special catalogue, containing the before generated requirements to computer system safety.

The next step is the creation of the security system overall specification, using the functional requirements (the list of functions, that security mechanisms should perform), the requirements for reliability (define the value of security mechanisms reliability and availability), the requirements for hardware (performance, price, etc.) And the last step is the creation of the updated catalogue with certificates for the adaptive security systems, which will be used for the future standards and RFC on the security mechanisms for computer systems and networks.

7. CONCLUSION

Today there are no uniform approaches to the development of information security mechanisms for computer systems and networks. This is caused by the fact that the design decisions should be based not only on the requirements to computer safety, but also on the interdependence between the information processing means and the information security mechanisms, on the functional requirements to the system and on the requirements to compatibility. In this paper we suggest an integrated approach to security mechanisms design. The integrated security mechanisms ensure proper access control to system information resources, effectively unify the all interactions in the security system, and also adapt the security mechanisms to the certain parameters of computer networks, that is important in practice.

8. REFERENCES

[1] V.P. Shyrochin, V.Ye Mukhin, A.V. Kulik. *The Design of the Information Security Mechanisms for Computer Systems and Networks*. "VEK+ ". Kiev, 2000. 112 p.

[2] A.Yu.Shcherbakov.*Computer Safety. Theory and Practice*. “Knowledge”. Moscow, 2001. 352 p.

[3] W. Stallings. *Cryptography and Network Security.* “Williams”. Moscow, 2001. 672 p.

[4] D.P. Zegzhda, A.M. Ivashko. *How to Design a Secured Information System?* “World”. Saint-Petersburg, 1997. 312 p.

[5] V.P. Shyrochin, V.Ye Mukhin, Hu Zhen Bin. The Condition Machine in the Users Authe-ntication Tasks in Computer Networks, *Managing Systems and Machines,* N 5 (2003). p.75 - 80.

[6] M. Crosbie, E. Spafford. Defending a Computer System Using Autonomous Agents, *Technical Report CSD-TR-95-022, Department of Computer Sciences*, Purdue University publishing. (1995). 107 p.

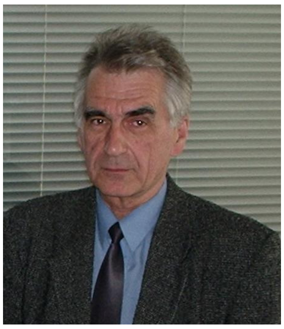
[7] S. A. Gurwitz. *The Measurement of Fiscal Capacity.* “Rand Corporation”. Washington, 1979.

[8] L.G.Labsker. Gurwitz Pessimism-optimism Common Criterion, *Financial Mathematics* (2001). p. 401 - 414.

[9] V.P. Shyrochin, V.Ye Mukhin. Formalization and Directed Adaptation of the Authenticating Mechanisms in Computer Networks, *Managing Systems and Machines*, N 5/6 (2000). p.59 -65.

[10] V.Ye. Mukhin. Means and Methods for Adaptive Safety Control in Computer Networks, *News of NTUU “KPI”. Series “Informatics, Control and Computer Systems”*, N 35 (2001). p.32 - 44.

[11] V.P. Shyrochin, V.Ye Mukhin, D.I. Kramar. The Risks Analysis in the Tasks of Safety Monitoring in Computer Systems and Networks, *Information Security* N 1 (2003). p.28 - 34.



***Loutsky Georgy Mikhailovich** was born in Kiev in 1938. Doctor of technical sciences, Professor, Head of computer engineering department of National Technical University of Ukraine “Kiev Polytechnic Institute”, where works since 1971, Vice-President of Ukrainian Academy of Informatics. The main scientific interests and researching fields: large scale high performance computer systems based on transputers technology; realization of computing processes in multi-computers environments with development of algorithms and software; static and dynamic scheduling for computing processes; methods and means for high performance computer systems and networks; parallel processing of information; methods and means for high performance distributed and cluster computer systems design; methods and means for computer systems safety providing. Graduated 3 doctors of technical sciences and 40 candidates of technical sciences (Ph.D.). Has 265 scientific publications, including 16 monographs and 25 patents.*

Shyrotchin Valerij Pavlovich *was born in t. Tulchin (Ukraine) in 1939. Doctor of technical sciences, Professor of computer engineering department of National Technical University of Ukraine "Kiev Polytechnic Institute", where works since 1962. The main scientific interests and researching fields: mathematical theory of Petri-networks in tasks of computer systems safety providing; software for dedicated computer systems; methods and software tools for computer-aided simulation of complex systems; processors and algorithms of digital signal processing; methods and krypton-algorithms for information security providing in computer systems. Graduated 8 candidates of technical sciences (Ph.D.). Has more than 150 scientific and literary publications, including 3 monographs and 20 methodical manual-text lectures.*

Mukhin Vadim Yevgenievich *was born in Kiev in 1971. Received Master of science degree in 1994 and Ph.D. in 1997 from National Technical University of Ukraine "Kiev Polytechnic Institute", where works since 1997. Associate Professor of computer engineering department of National Technical University of Ukraine "Kiev Polytechnic Institute". The main scientific interests and researching fields: methods and means for users and messages authentication procedures in computer networks; theory of monitoring of safety in computer systems and networks; theory of safety and reliability of software; methods and means for high performance distributed computer systems design, methods and means for cluster computer systems safety providing. Has more than 80 scientific publications, including 1 monograph and 5 methodical manual-text lectures.*