Journal scientific and applied research №1, 2012
Association Scientific and Applied Research
International Journal

ISSN 1314-6289

Original Contribution

АЛГОРИТЪМ ЗА ЗАЩИТА НА ИНФОРМАЦИЯТА В АВТОМАТИЗИРАНИ СИСТЕМИ

Веляна М. Желязова, Иван Б. Николаев
Адрес: Гр. Русе, ул. "Ниш" № 32, вх. 1., ет. 4, ап.8 , phone 0883347201, email: mjeliazov@uni-ruse.bg

ALGORITHM FOR INFORMATION PROTECTION IN THE AUTOMATED SYSTEMS

Velqna M. Zhelyazova, Ivan B. Nikolaev

Abstract: *This scientific report proposes Algorithm to protect information from unauthorized access (IPUA) in the automated systems (AS) with integrated procedures of analysis and synthesis. Currently, the insurance of the information safety (IS) in the automated systems for information processing in the management of different objects becomes a major importance. These objects include: telecommunication systems, banking systems, systems providing the work of the atom electro stations, systems for management of sea, air and land transport, systems for processing and storing of confidential and secret information [1, 2, and 9]. The high usage of local, corporative and global networks with the appliance of open protocols for data transmission intensifies the problem with the information protection.*

Key words: *information protection, Structure synthesis, administrators and services*

There are special systems for information protection: problem-based systems and subsystems containing technical and software protection resources [1, 2, 9]. The system for information protection (SIP) represents a combination of bodies, used technology, objects for protection, organized and functioning according to the rules, stated by the matching legal, organization-regulating and normative documents [10]. The issue for information protection from unauthorized access is a part from the general one, regarding information security that is why within the systems for information protection (IP), there appears to be a new structure. This is a complex of organizational criteria, program-technical (including cryptographic) resources for information protection in the ACS. The main problems for providing information security in the ACS that need to be solved during the development of the protection systems can be separated [1, 2, 9]:

1. Providing security of the data, especially when it is stored, processed and transferred through the connecting channels (by cryptography, access division, etc.);
2. Providing security of the machine resources(specialized verifications of the integrated devices, special researches of the peripheral electromagnetic emissions and

directing of the program provision, additional verifications for absence of hidden or non proved functions);

3. Creating a program-machinery resources for protection(for a separated workplace, network and internet work workplaces);

4. Developing of the already mentioned directions with organization technical measures within the system providing information security. For the creation of systems for information protection, the nature of possible threats, the forms and conditions in which they would appear in the ACS, need to be defined. The solution to this issue might be expressed by reducing the whole variety of threats and their methods of impact to their simple forms [1, 2, and 9]. The object considered for protection is the calculating system which could be a part from a big ACS [1, 2, and 9]. This way, [2…4] the SIP is a complicated organization technical system including different program-technical and program and methodical complexes with a big number of various parameters. That is why the creation of a SIP demands the developing of a matching mathematical and program provision, designed for a system for automated projecting (SAP) and for increasing the efficiency of the information security resources. In this case, it needs to be taken into account the big amount of issues that can be resolved by program resources for information protection. That is because of their universality, reliability, simple practical putting into effect and a possible modification. AP of SPUA must include subsystems and resources that support the interconnected development of program machine complexes. The order of projecting SAP of systems for protection from unauthorized access is characterized by multi-staging and includes a whole succession of analysis and synthesis procedures. In the practice, it is usually necessary the solution of two major problems-the synthesis of a system for information security in the process of creating ACS and the analysis of the efficiency of this system during its functioning.

- Projecting of a SIP together with the developing of the protected ACS itself by beginning from the formulating of the general conception at all stages: developing the technical proposal; technical project; preparing work documentation; verification and transmitting from the commissioner. The non-fulfillment of this principle might lead to a low efficiency of the protection, deflection of additional resources and increasing the losses upon providing the demanded stage of protection. This way, the requirements for SIP form a hierarchical system and they must be included in the general technical assignment of ACS and in the separated technical assignments of the subsystems.

- Development of the SIP must be accomplished by specialists with demanded qualification that would provide a complex solution to the problems of the IS, development of the program insurance and the program technical complexes, organization and system issues. The systems need to follow

the requirements for efficiency with minimum excess, increasing their reliability.

• An additional requirement is providing privacy of the documentation and official information. The structure of the SIP projecting process is shown in Figure1, where an algorithm with procedures of synthesis and analysis is illustrated. Corresponding to the algorithm, in the process of developing SIP there might be separated the following stages:

1. Analysis of the informational technical characteristics of the ACS and formation of a multitude of out coming data for development of SIP-the number of demanded parameters is defined.

2. Analysis of the requirements regarding the information safety of the ACS, formation of the technical assignment of SIP, formation of amount of indicators for its efficiency and defining of limits providing the minimum acceptable level of protection.

3. Defining and analysis of the possible channels for unauthorized access-searching for all possible channels responsible for leaking of information. Making a list, consisting of all threats for the information and composing their mathematical models.

4. Forming of a list of potential transgressors-based on the normative documents, literary sources, accumulated experience, and taking into consideration the specific work conditions of ACS, a model of the potential transgressors is formed, and a sub-majority of all channels for informational leaks is determined.

5. Forming of a list of major requirements for the resources for IP - it's made after analyzing of the possible channels for informational leaks, the potential threats and transgressors. The resources for IP have to ensure collapse of the existing channels and protection of appearance of new channels for informational leaks.

6. Selection or developing of program resources for IP-selection of the demanded software from the existing program products and creation of new ones in order to increase the reliability of the SIP.

7. Selection of technical resources for IP. These resources must fulfill exact requirements, providing the necessary protection at a machine level. These technical resources must fulfill the program resources for IP and provide compatibility and stable functioning of the programs for IP.

8. Structure synthesis and optimization of the composition of the SIP is accomplished, in order to ensure full coverage of all channels for informational leaks.

9. Analysis and evaluation of the criterion efficiency of the resources complex for IP. If any defects of the SIP are detected, a method for their removal is offered.

10. Completing (modifying, adapting) and parametric optimization of the resources complex for IP-removing the defects and adaptation of the conditions for functioning.

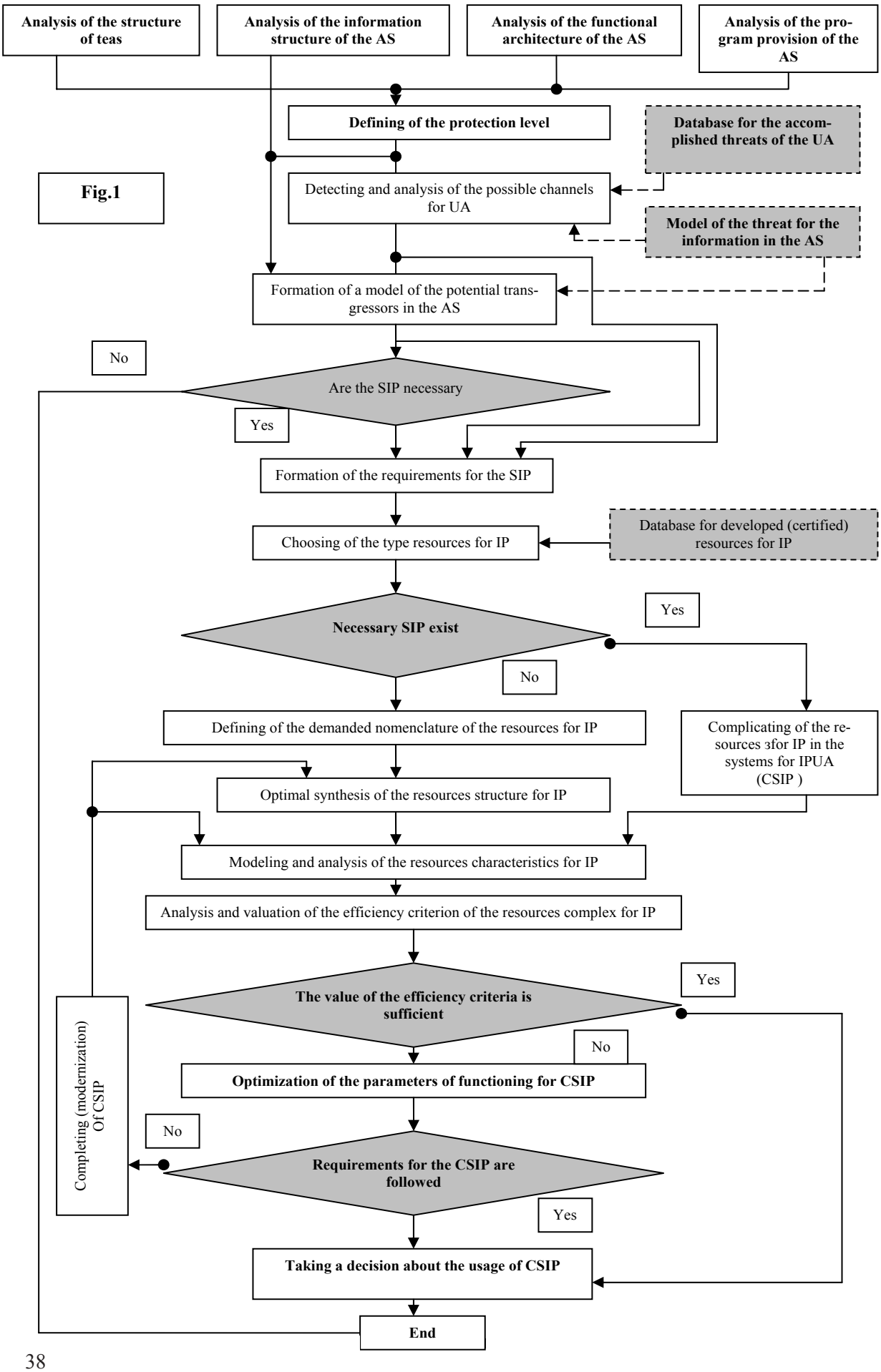
Analysis of the structure of teas
Analysis of the information structure of the AS
Analysis of the functional architecture of the AS
Analysis of the program provision of the AS
Defining of the protection level
Database for the accomplished threats of the UA
Detecting and analysis of the possible channels for UA
Model of the threat for the information in the AS
Formation of a model of the potential transgressors in the AS
No
Are the SIP necessary
Yes
Formation of the requirements for the SIP
Choosing of the type resources for IP
Database for developed (certified) resources for IP
Necessary SIP exist
Yes
No
Defining of the demanded nomenclature of the resources for IP
Complicating of the resources for IP in the systems for IPUA (CSIP)
Optimal synthesis of the resources structure for IP
Modeling and analysis of the resources characteristics for IP
Analysis and valuation of the efficiency criterion of the resources complex for IP
The value of the efficiency criteria is sufficient
Yes
No
Optimization of the parameters of functioning for CSIP
No
Requirements for the CSIP are followed
Yes
Completing (modernization) Of CSIP
Taking a decision about the usage of CSIP
End

Fig.1

Complicating and evaluation of the efficiency of the program technical complexes for IP-integrating of the subsystems and the elements for IP and ensuring information compatibility, centralized control and management by the automated workplaces of the administrators and services for IS; complex evaluation of the efficiency of the whole program technical complex for IPUA, the stage of protection from unauthorized access and the work stability in critical situations. In case of detecting any defects, the components of the system get additional completing and their interaction gets corrected, separate resources for protection get changed, a duplicate of the most often appearing threats and channels for unauthorized access is integrated. Through the implementing of the described procedures, a program technical complex for IP might become highly resistant to preliminary assigned outer and internal influence. The analysis of the actual content at these stages allows to conclude that they include not only poorly formalized tasks requiring qualified professionals to solve them, attracting experts using heuristic methods and approaches, but also tasks which can be formalized in within the structural synthesis, optimization and parametric identification by attracting basics of mathematical programming. One of the major issues is the choosing from the multitude of available resources that allow forming the structure of a certain system for information protection ensuring the coverage of all open channels for informational leaks. Usually, the multitude of protection resources at a network stage includes the following: control of the access to the object territory, the server premises and the workstations; control of the installations opening; encoding the information for service access to the server and the separate personal computers at the workstations; understanding, distinguishing and control of the access to the resources of the network, the operating systems, the database, the program insurance and the subscribers' data; decreasing the noise level and the number of operations responsible for transforming the information; control of the entireness of the informational program surroundings at a workstation and used software insurance level.

The choosing of the necessary resources from the multitude of accessible ones represents a problem regarding an optimal structure synthesis of a complex system [2-4], aiming maximum following of the requirements for SIP. These requirements are placed at the base of the matching objective functions and restrictions. That is why the choosing of the matching resources is a problem of a primary importance because the results of its solution are out coming base for the solution for all this upcoming problems, especially the synthesis and the optimization.

Specific quarrymen's for means of IS, determined by the specifics of digital information processing, are determined by the following factors: nature of the processed information, downtime of the information in ACS, the volume of information, structure of ACS, the type of the protected infor-

mation, technology used in processing, nature of the calculation process in the ACS, stage of the lifecycle of the ACS. Requirements dictated by the technological schemes for automated processing in the ACS can be brought to the level that in active condition the ACS must be provided with protection in all areas of automatic processing and in all modes. From a standpoint of organization of the calculation process required in the ACS, protection should be provided at each level of automation of processing in all forms of interaction between subscribers by means of automation in all operating modes of the complexes by means of automation.

In conclusion, it might be stated that the formation of the multitude of requirements regarding the resources for IP which are adequate to their purpose and level of disposition of the ACS to the security level, is the most important problem, defining the characteristics of the projected system for protection and the necessary resources.

Referens

[1]. Gerasimenko, VA Information Security in the automated data processing systems. Book 1 M.Energoatomizdat., 1994.

[2]. Methods and tools for performance analysis of software for the design of information security. O. Makarov and others, Astrahan., Vilnius Gediminas Technical University, 2002.

[3]. Norenko IP, VB Manych Fundamentals of the theory of design CAD. Moscow: Higher School., 1993.

[4]. Avtomatizirovannoga system design. Ed. Norenkova IP and other Moscow, V.Shkola., 1190.

[5]. State Technical Commission of Russia. Guidance document. Protection against unauthorized access to information. Terms and opredeleniya.M. : 1992.

[6]. State Technical Commission of Russia. Guidance document. The concept of protection of computers against unauthorized access to information. Moscow, 1992.

[7]. State Technical Commission of Russia. Guidance document. The automated system. Protection against unauthorized access to information. Classification of automated systems and requirements for information security. Moscow, 1992.

[8]. State Technical Commission of Russia. Guidance document. Provisional Regulations on the organization of the development, manufacture and operation of software and technical means of protection against unauthorized access to information in automated systems and computer equipment. Moscow, 1992.

[9]. Zegzhda DP, Ivashko AM Fundamentals of Information Systems Security. M. Hot Line - Telecom, 2000.

[10]. GOSTR 50 922 - 96 standardized terms and definitions in the field of information security.