Journal of Computer Networks, 2014, Vol. 2, No. 2, 18-22
Available online at http://pubs.sciepub.com/jcn/2/2/3
© Science and Education Publishing
DOI:10.12691/jcn-2-2-3

Selection Criteria of the Tools of Information Security from Unauthorized Access into Computer Systems of Different Classes

Oleksiy Gavrylenko, Sergiy Gnatyuk*, Dmytro Matviiv

IT-Security Academic Department, National Aviation University, Kyiv, Ukraine
*Corresponding author: s.gnatyuk@nau.edu.ua

Received May 30, 2014; Revised June 02, 2014; Accepted June 03, 2014

Abstract The authors of the article proposed the definition of selection criteria of technical products protection of information from unauthorized access in automated systems of different classes based on the analysis and synthesis of classifications, characteristics and requirements to the known products for the purpose of forming the appropriate method of choice product protection.

Keywords: *threat, information, automated system, technical protection of information, complex system of information security, information security product, unauthorized access, technical task, software, criteria of choice, method*

Cite This Article: Oleksiy Gavrylenko, Sergiy Gnatyuk, and Dmytro Matviiv, "Selection Criteria of the Tools of Information Security from Unauthorized Access into Computer Systems of Different Classes." *Journal of Computer Networks*, vol. 2, no. 2 (2014): 18-22. doi: 10.12691/jcn-2-2-3.

1. Introduction

With the development of information technology the problem of security of information during processing, transmission, storage in the information (automated) and telecommunication systems (hereinafter - AS) is becoming more widespread, the most effective way is to ensure an appropriate level of protection of such information, that is preventive measures of identifying and the prevention of danger, which are aimed at creating the environment where the implementation of dangers not possible or losses from their realization are minimal.

Implementation of these measures in terms of technical information security (hereinafter - TIS) is based on the use of the material and technical basis of sound consisting of remedies for general and special purpose in Ukraine is sufficiently developed. The modern market is full of domestic and foreign production. Thus, the list of general purpose tools that allowed for providing of TIS, the need for protection of which is determined by the legislation of Ukraine (hereinafter - the List) [1] contains more than 260 items of protection of domestic and foreign production.

The law of Ukraine "About data protection in information and telecommunication systems" [2] and other normative legal acts of Ukraine in the field of information security is established that government information resources or classified information, the protection of which is set by law, have to be processed in the system of using complex system of information security (hereinafter - CISS) in the confirmed accordance with the requirements of normative documents of the TIS system (hereinafter - ND). During the creation of CISS in AS of any class the formation of appropriate requirements to the providing of the information protection against the unauthorized access (hereinafter - UA) are performed, the choice of security tools is based on these requirements which are underlying in the formation of the criteria for their selection. Selection can be carried out with the List of [1] as well as among any other existing means, technical characteristics of which will ensure the implementation of the functional security services in AS described in the ND TIS 2.5-004-99 [3].

Problem definition. The current diversity of security tools makes the choice of technical security information tools against unauthorized access (hereinafter - SIT against UA) during the construction of the CISS in AS quite a challenge, since before making such a choice a CISS developer has to know what criteria the choice has to be made on which characteristic options and parameters of tools to focus on and what is appropriate to draw attention to for a particular AS.

Currently there are a number of known approaches, that means that tools of TIS against UA are classified according to certain features and characteristics, including statutory domestic [4,5,6,7] and international [8,9] standards.

Moreover, among these approaches there is no general set of features that makes it possible to give the most complete description of any SIT against UA, required to use it in order to resist currently important information threats in the AS. This features may be the basis for the definition and explanation of choice of the security tools criteria in the construction of CISS in AS.

The aim is to identify the selection criteria of technical security information tools against unauthorized access to AS of different classes based on the analysis and synthesis of classifications and descriptions of known tools to form an appropriate method of optimal choice of security tools.

The method of choice will be formed on the basis of the selected criteria with the purpose of optimization of such choice and proper reduction of time on its lead through. The programmatic module, realization of which will diminish the intellectual loading on developer of CISS in relation to the search and comparison of deference facilities must complete the creation of method.

This work is exactly devoted to the determination and generalization of the choice criteria of SIT against UA.

2. Main Part

Requirements to the functional composition, order of development and implementation of hardware which provide safety of information in the process of its treatment in AS are laid out in a technical specification of CISS, that is developed in accordance with ND of TIS 3.7-001-99 “The methodical guidelines on the development of technical specification creation of the complex system of information security in automated system” [10]. The initial data for the development of TT of CISS is functional profile security of CS against UA. The functional profile of information security in particular AS is determined as a result of lead through of analysis of threats and estimation of risks or is selected on the basis of class in accordance with ND of TIS 2.5-005-99 “Classification of automated systems and standard functional profiles of the machined protection of information against unauthorized access” [11].

Confirmation of accordance to CISS in AS with the requirements of normative documents of TIS as the resulting stage of creation of the complex system has to be carried out exactly in the part of TT requirements. Confirmation procedure of accordance is a state examination in the field of TIS [12].

Therefore the determination of the choice criteria of SIT against UA must help the developer of CISS in achievement of such accordance by the most optimum way.

Let us consider the main known approaches (sources), that include criteria for evaluating remedies, some features, requirements and specifications on the basis of which selection criteria of SIT against UA can be formulated.

ND of TIS 2.5-004-9. “Criteria for information security evaluating in computer systems against unauthorized access” [3].

This regulatory document sets the criteria for assessing the security of information processed in AS against UA.

The document is the methodological basis for the determining the requirements of the information protection in computer systems against UA; creation of the protected AS and security tools against UA; evaluation of information security in the AS and their suitability for processing of the information requiring protection.

Criteria provide:

The comparative scale for the estimation of reliability of information security mechanisms against the unauthorized access, implemented in AS.

Base (guidelines) for development of the computer systems where the functions of information security must be implemented.

AS in the document is considered as a set of functional services that in turn is a set of features to withstand a certain set of four basic types of threats: threats to confidentiality, integrity, availability, and observation.

In the process of assessing the ability of automated systems to protect information against UA the requirements of two types are considered: the requirements for protection functions (security services) and requirements for guarantees.

Requirements to the services of safety, that provide protection against the marked threats, are described by the functional criteria of four groups: criteria of confidentiality, integrity, availability, observation. Every criterion is corresponded by the set of functional services of different levels. On the basis of existent requirements in relation to the protection of certain information against certain threats the functional profile of security is consisted of the marked services.

Requirements for the guarantees. The criteria of guarantees that include requirements have 7 hierarchical levels. The hierarchy of guarantees levels removes the gradually increasing measure of definiteness in the fact that service realized in AS allow to resist against certain threats, in turn that mechanisms that will realize them are correctly implemented and can provide the level of information security expected by a consumer during exploitation of AS.

Thus, the evaluated for compliance with the specified requirements of protection security tools will be characterized by:

- The implemented functional profile of protection;
- The level of functional guarantees of security services.

The first characteristic is the initial data for the development of TT for CISS [13], and the second one provides an advantage over other tools that, for example, have a lower level of guarantee or a level is not determined. These specifications should be classified as the main criteria for selecting information security against UA.

ND of TIS 2.5-005-99. “Classification of automated systems and standard functional profiles of the machined protection of information against unauthorized access” [11].

This document establishes principles of classification and formation of the AS standard functional profiles processed information security against UA and provides regulatory and methodological framework for the selection and implementation of information security requirements in AS.

On the totality of characteristics of AS three hierarchical grades (hardware configuration and operating and their physical location, the number of different categories of information processed, the number of users and types of users) are identified, the requirements for the functional components of remedies of which are significantly different:

- AS Class 1 –onemachine with oneuser complex, which processes the information to one or more categories of confidentiality;
- AS Class 2 –localized multiplayer multicomputer complex that processes information of various categories of confidentiality;

- AS Class 3 –distributed multiplayer multicomputer complex that processes information of various categories of confidentiality.

Accordingly, data protection must be chosen depending on the class of AS for which they are designed.

Statement on the State examination in the field of technical protection of information [13].

State examination in the field of TIS (further - examination) is made to research, test, analysis, and evaluation of examination for compliance with regulatory requirements of TIS and possibilities of their use for TIS.

Objects of examination are comprehensive information security in systems in automated systems and hardware and software tools that implement functions of TIS. Examination of such facilities is carried out by expert testing. According to the results of the examination the expert opinion is recorded on the proofing tool (in our case - to SIT against UA).

Registered expert opinion on the product confirms its compliance with regulatory requirements of TIS and its possible use for the technical protection of information (especially regarding the information that requires protection under the law). Also, the presence of an expert opinion on the product of TIS simplify the state examinations CISS in AS by eliminating the need for confirmation during its performance of evaluated services of safety and warranty of tools.

Therefore, the presence of this opinion is doubtless an advantage that should be considered when selecting SIT against UA by the developer of CISS.

Security tools of TIS, that received an expert opinion are included in the List. [14].

The list is formed according to the provisions of Section 17 of the Protection of Information Technology in Ukraine [1] and is intended for use by entities of TIS in the development, modernization and implementation of TIS objects in information activities (OIA) and CISS in AS.

Use of the List [1] in the development, modernization and implementation of CISS in AS does not dismiss from the assessment need of compliance achieved level of information as required by ND TIS which is made by examination of CISS in AS [9] however, as noted above, simplifies examination.

Currently the list is the primary source of pre-selection SIT against UA during construction of CISS (final choice can be based on technical and operational documentation for the tool provided by the manufacturer). For each remedy information against unauthorized access list contains the information about the implemented functional profile and the level of security guarantees for the implementation of functional safety services. SIT relation to certain assets, credit facilities, or regular components (hardware or software) may also be determined on the list.

GOST 3396.2-97. "Information Security. Technical protection of information. Terms and definitions" [15].

The document provides the following definition:

- technical means of protection; protected by technical means - the technical means, which in addition to the basic assignment function provides information security against threats;

- means of technical protection of information - the device and (or) software tool which main purpose is the protection of information against threats.

ND of TIS 3.6-001-00. "Technical data protection. Computer systems. The procedures of establishing, implementing, maintaining and upgrading of technical protection of information against unauthorized access" [16].

This regulatory document establishes uniform requirements for procedure development, implementation, maintenance and modernization of technical protection of information against unauthorized access in the AS and protected against UA components of computing systems.

According to [16] means of technical protection of information against UA– it is a software, hardware or software-hardware tool that is created as a separate product manufacture, has the necessary software and / or design documentation, and provides its own or in combination with other means of protection against threats UA for information on the speakers, or used to monitor the effectiveness of information against unauthorized access to such systems.

Therefore, when choosing remedies its implementation method should be considered: software, hardware, hardware and software, and the ability to use it - either alone or in combination.

ND of SIT 2.7-009-09. "Guidelines for the assessment of functional security services in the mass of information security in computer systems against unauthorized access" [17].

The document provides the following definition:

tools of technical protection of information against unauthorized access –the definition is similar to [16] (excluding the possibility of its use to monitor the effectiveness of information);

protected against unauthorized access component of a computer system (hereinafter - OS) - software, hardware or software and hardware product, where in addition to the functions provided for the main purpose, the information security threats against unauthorized access is provided.

Summarizing the information and determinations considered in the last 4 sources [1,15,16,17], the authors offer the following selection criteria of SIT against UA, "the way to use":

- A separate tool (a tool (including protected against unauthorized staff component of the OS), which is produced as a separate product of manufacturing protection against threats);

- A set of tools (a set of individual agents (including, protected against unauthorized staff component of the OS) used in combination to protect against threats)

"The primary purpose":

- The protection of information against UA threats;

- In addition to the functions provided for the main purpose, the information security functions against UA threats are provided (protected against UA staff component of the OS).

The objects of protection.

Depending on the main basic types of information, which needs to be protected, and according to the list of [11] one can identify the following facilities protection: text, graphics, video and audio files; spreadsheets; database and so on.

The relevant criteria will provide a means choice, based on the protection of objects that will be handled in the AS.

Environment of SIT operation against UA.

It is well known that any software used in the AS has some limitations as to the compatibility with the operating system (hereinafter - OS) (of course, if it is the operating system with the functions of protection), under control of which it will work and the hardware on which it will be installed. There are also limitations in relation to other software, which is compatible with the security software, will operate in the system. Of course, the market uses a large number of operating systems and other software specific versions, so the choice of remedy should be made depending on whether the set (selected for the installation) is software, whether it is selected simultaneously with the choice of remedy.

Therefore, during the formation of the criteria for selecting of the remedies it is proposed to pay attention to the restrictions on their compatibility with other software, especially OS.

Market value of the product.

An important selection criterion of the technical SIT is its cost. In general, the amount of the price of tools can be significant and the availability of value added tax, which is usually subject to the sale of goods in Ukraine (paragraphs 14.1.191 Pkt. “a” Section 185.1 of the Tax Code of Ukraine) [18], does not improve the situation.

However, the choice of means must depend primarily on the requirements of the protection given to ensure the completeness of its protection (at least when it comes to the information that requires protection under the law of Ukraine). In particular, this approach is determined by GOST 3396.0-96 “Information security technical protection of information. Key provisions” [19] according to which information security measures must ensure the given effectiveness of the protection to the set level. It is only in the second stage the protection depends on the financial capacity of the owner or developer of the AS.

In any case if more than one remedy is available on the market that meets the stated requirements, the choice of means is appropriate to carry on the criterion of the lowest price. This approach, of course, will provide the cost savings, especially when it comes to public funding.

Technical and operational documentation for a TIS.

This documentation is formed by the developer (manufacturer) of tools in general (for complex software) as an example of complex software - local systems of information protection LOZA-1) [20] may comprise means for passport, general product, instructions of the security administrator, system administrator and user, description of the software, the user manual of the individual programs that are included in the product.

Passport and general description of the product should contain basic information about it, including: functional profile security, level of functional guarantees of security services, information about class AC, for use in which it is designed, facilities protection, environment protection operation of the means (compatibility with the software), requirements for support (for the software - the amount of RAM memory and on the hard disk), data on the presence of conformity with regulatory requirements of TIS.

This main data and other data of the above documents complement data of list [14] and are the main source of information about the product during its final selection.

That technical and operational documentation of SIT against unauthorized access must include the vast majority of basic data needed to select the remedy against unauthorized access and comply with all the major (except for the cost) considered above criteria for this choice.

The required documentation for a composition largely depends on the purpose, method, characteristics of the specific SIT against unauthorized access, requires further study and will be taken into account during the development of the method of optimal choice of vehicle.

Table 1. Criteria of choice of SIT against UA

№	Criteria	Characteristics (destination) of product Satisfying the criterion
1	Implemented security functional profile	Availability of implemented security functional profile(criteria that are present in ND TIS 2.5-004-99 [3]),which provides the ability to protect against threats to confidentiality, integrity, availability, observation (individually or collectively).
2	Class AS, which uses a product	For use in AS of Class 1, 2, 3 or for use few classes (ND TIS 2.5-005-99 [11]).
3	Objects of protection	The list of objects of protection that are processed in AS alone or in combination: texts, graphics, video and audio files; spreadsheets; database and so on.
4	Software compatibility	Restrictions on product compatibility with operating systems and other software used in the AS.
5	Requirements for technical support	- Amount of RAM; - The amount of memory on your hard disk.
6	Method of use	individual product (product (including protected against UA staff component of OS), which is created as a separate product production against protection of dangers); complex of products (set of individual products (including protected against UA staff component of OS), used in combination to protect of dangers).
7	Availability of technical and operational documentation of product	Documentation, including: passport of product, general description of the product, manuals of security of administrator, system administrators and users, description of software, user manuals of the individual programs that make up the product and so on.
8	The level of functional guarantees of security services	G1, G2,…, G7 (ND TIS 2.5-004-99 [3]).
9	The presence of attestation of conformity in ND TIS	Having a document that certifies the conformity of product of TIS requirements of ND TIS (expert opinion or certificate of conformity of TIS against UA
10	Price range of product protection	The cheapest among the products that ensuring full implementation of the requirements for protection laid down in the TT for CISS in AU.
11	External environments	Ability warranty (post-warranty) service, availability requirements for personals, the possibility of extending the license and so on.
12	Method of implementation	Software, hardware, hardware and software
13	The main purpose	the protection of information from UA; In addition to the functions provided for the main purpose of information security against UA (protected against UA staff component of a computer system).

On the results of the definition of the criteria selection of SIT against unauthorized access during the development of the AS CISS the generalized criteria table was formed (Table 1). Using these criteria based on the requirements of the TT for CISS and technical and operational documentation for product information security professionals can choose the protection they need. Additional consideration to criteria that, in the opinion of the author do not require a separate study are also included to the Table 1.

The criteria in Table 1 are in descending order, according to the authors, the degree of importance in relation to the performance by means of functions protecting information against unauthorized access.

3. Conclusion

This paper reviews the main known approaches that contain criteria for assessing technical protection of information against unauthorized access, their individual characteristics, their requirements and specifications. Based on the analysis of the data it was set and generalized the selection criteria of SIT against unauthorized access to computer systems of different classes.

The result should simplify for the developer of CISS in the AS searching of the remedies necessary to ensure compliance with the requirements of AS to protect information generated in the Terms of Reference for the creation of CISS. For example, the developer can use the general information contained in the criteria of required features, functions the characteristics, the purpose of these tools, etc. at which one need to pay attention to when choosing them.

Formed criteria and their ranking in descending order of importance in relation to the implementation of UA SIT security features can be the basis for further development of the method of selecting the appropriate remedies in order to optimize this choice.

The compiled list of criteria is not exhaustive. It can be expanded and supplemented on the basis of improvement requirements and rules of SIT against unauthorized access to the AS, market development funds and, therefore, the emergence of new settings and features, as well as the parameters and characteristics of specific existing remedies in more detail on the results of their research.

References

[1] Decree of President of Ukraine, Position number 17 is about a technical information security in Ukraine, List of tools of the general setting, which are selected for providing of technical information security, necessity of guard of which by the legislation of Ukraine, 27 Sep 1999.

[2] Law of Ukraine, About information security in informatively telecommunication systems, 5 Jul 1994. [Online] Available: http://zakon4.rada.gov.ua/laws/show/80/94-вр.

[3] Order number 22 of the Department of the special telecommunication systems and information security of Ukraine Service, ND TIS 2.5-004-99. Criteria of estimation of protection of information are in the computer systems from an unauthorized access, 28 Apr 1999.

[4] I.Z. Duchyak, Creation of classifiers, 2010. [Online] Available: http://pidruchniki.ws/1633082637655/logika/stvorennya_klasifikatoriv.

[5] L.I. Abrosymov, A.Y. Koablev, Methods and security information tools, [E-book] Available: http://www.melnikoff.com/yuriy/posobie.htm.

[6] Order number 472 of the Administration of Government service of special communication and information security of Ukraine, ND TIS 1.5-002-2012. Classifier of tools of technical security information, 29 Aug 2012.

[7] I.I. Simora, O.V. Gavrylenko, Classifier of tools of information security in informatively telecommunication systems, The 3rd international Scientific Conference ITSEC, National aviation university, 145.

[8] GOST P ISO/MEC 12182-2002, Classification of programmatic tools, 01 Dec 2002.

[9] ISO/IEC 15408-1:2009, Information technology -- Security techniques, Evaluation criteria for IT security -- Part 1: Introduction and general model.

[10] Position number 1299 about a technical information security in Ukraine, ND TIS 3.7-001-99. The methodical pointing is in relation to creating of requirement specification on creation of the system of information security of automated system, 27 Sep 1999.

[11] Order number 22 of the Department of the special telecommunication systems and information security of Ukraine Service, ND TIS 2.5-005-99. Classification of AS and standard functional types of protected of the processed information is from an unauthorized access, 28 Apr 1999.

[12] Order number 93 of the Administration of Government service of special communication and information security of Ukraine, Position about state examination in the sphere of technical information security, 16 May 2007.

[13] State standard of Ukraine, DSTU 3974-200. The system of development and imputing of products is on a production: Rule implementation of experimental and designer work, 01 Jun 2000.

[14] List of facilities of TIS, which have an expert conclusion about accordance with the requirements of technical information security, [Online] Available: http://dstszi.kmu.gov.ua/dstszi/ control/uk/publish/. /.[Accessed May. 2, 2014].

[15] Order number 200 of State standard of Ukraine, DSTU 3396.2-97. information security. Technical information security. Terms and determinations.11 Apr 1997.

[16] Order number 60 of the Department of the special telecommunication systems and information security of Ukraine Service, ND TIS 3.6-001-2000. Technical information security. Computers systems. An order of creation, introduction, accompaniment and modernization of facilities of technical information security, is from an unauthorized access, 20 Dec 2000.

[17] Order of the Department of the special telecommunication systems and information security of Ukraine Service, ND TIS 2.7-009-09. Guidelines for the evaluation of functional services security tools protecting information in computer systems from unauthorized access.

[18] Tax Code of Ukraine number № 2755-VI., 02 Dec 2010. [Online]. Available: http://zakon4.rada.gov.ua/laws/show/2755-17/. [Accessed May. 2, 2014].

[19] State standard of Ukraine, DSTU 3396.0-96 Information Security. Technical protection of information. The main provisions, 01 Jan 1997.

[20] Information security tool, [Online] Available: http://avtoprom.kiev.ua/avtoprom/ua/content/.