Model and Method for Identification of Functional Security Profile

Anatolii Davydenko[1], Oleksandr Korchenko[2], Olena Vysotska[3], Ihor Ivanchenko[4]

[1,2,4] *National Aviation University, Liubomyra Huzara ave. 1, Kyiv, 03058, Ukraine*
[3] *Pukhov Institute for modeling in energy engineering of NAS of Ukraine, General Naumov str. 15, Kyiv, 03164, Ukraine*

Abstract

One of the key tasks during the state examination is the identification of the functional security profile. During the examination, the types of information that is processed and the risks of its loss, modification or disclosure are evaluated. For this, the functional security profile is being built. To solve the problem of identifying the functional security profile, it is necessary to: determine the levels of functional security services, implemented comprehensive information security systems of the object of examination; determination of the completeness and consistency of the profile; identification of the description of the functional security services in the source documents. The paper proposes a model of parameters for identifying the functional security profile in computer systems. A definition is given for the sets of criteria, their elements and levels. All this made it possible in a formal form to form the necessary set of quantities for the implementation of the identification of functional security profile in the computer systems. The development of these works is the development of a method for identifying functional security profile. This will automate the determination of the requirements of the regulatory document regarding the protection functions (security services) and guarantees, which will be done in subsequent articles.

Keywords

comprehensive information security systems state examinations, functional security profile, information security criteria, computer systems.

1. Introduction

One of the key tasks during the state examination is to identify the functional security profile. During examination evaluated the types of information [1-8], which is processed in the system and the risk of its loss, modification or disclosure. For this purpose, a functional security profile (FSP) is built which contains the lists of functional security service (FSS) and levels that are needed to ensure an acceptable level of information security.

Exactly FSP is the key element of public examinations and its analysis on accordance to the normative document is one of major tasks.

For the decision of task of FSP authentication, it is necessary to carry out: determination of FSS levels, implemented FSP examination object; determine completeness and consistency profile; FSS describe the identification in the original documents. To determine the completeness and consistency of rules to consider construction of FSP (see [9]), and automation of this process contacts with corresponding rules.

For the decision of task proposed model parameters for identifying the FSP in computer system (CS) and FSP identification method.

2. Determining the criteria set

As it's known [9], the criteria reflect methodological framework for determining requirements of information security in of computer systems against unauthorized access,

III International Scientific And Practical Conference "Information Security And Information Technologies", September 13–19, 2021, Odesa, Ukraine
EMAIL: davidenkoan@gmail.com (A. 1); icaocentre@nau.edu.ua (A. 2); lek_vys@ukr.net (A. 3); igor-p-l@ukr.net (A. 4)
ORCID: 0000-0001-6466-1690 (A. 1); 0000-0003-3376-0631 (A. 2); 0000-0002-9543-1385 (A. 3); 0000-0003-3415-9039 (A. 4)

the creation of protected CS and protection against unauthorized access, evaluation of information security in the CS and its suitability for the treatment of critical information (information that requires defense).

Given the above, let's form the set of all criteria for information security

$$МК = \left\{ \bigcup_{q=1}^{w} МК_q \right\} = \{МК_1, МК_2, .., МК_w\}, \quad (1)$$

where $МК_q \subseteq МК$ $(q = \overline{1,w})$ – q-th element of set of criteria МК, and w - its count.

3. Determining of element of the criteria set

Next, on the basis of (1) we define the elements of the $МК_q$-th set of criteria

$$МК_q = \left\{ \bigcup_{e=1}^{w_q} МК_{q,e} \right\} = \{МК_{q,1}, МК_{q,2}, .., МК_{q,w_q}\}, \quad (2)$$

where $МК_{q,e} \subseteq МК_q$ $(e = \overline{1,w_q})$ – e-th element $МК_q$ - th set of criteria, and w_q its count.

Thus, (1) with respect to (2) we present in the following form:

$$\begin{aligned} МК &= \left\{ \bigcup_{q=1}^{w} МК_q \right\} = \left\{ \bigcup_{q=1}^{w} \left\{ \bigcup_{e=1}^{w_q} МК_{q,e} \right\} \right\} = \\ &= \{\{МК_{1,1}, МК_{1,2}, ..., МК_{1,w_1}\}, \\ &\{МК_{2,1}, МК_{2,2}, ..., МК_{2,w_2}\}, ..., \\ &\{МК_{w,1}, МК_{w,2}, ..., МК_{w,w_w}\}\}. \end{aligned} \quad (3)$$

4. Determination of levels of elements of the set criteria

Next, on the basis of (3) we define the level of each element $МК_{q,e}$ - th element $МК_q$ - th set criteria.

$$МК_{q,e} = \left\{ \bigcup_{y=1}^{w_{q,e}} МК_{q,e,y} \right\} = \{МК_{q,e,1}, МК_{q,e,2}, .., МК_{q,e,w_{q,e}}\}, \quad (4)$$

where $МК_{q,e,y} \subseteq МК_{q,e}$ $(y = \overline{1,w_{q,e}})$ – y-th level $МК_{q,e}$-th element $МК_q$ - th set criteria and $w_{q,e}$ its maximum level.

Thus, (3) with respect to (4) has the form:

$$\begin{aligned} МК &= \left\{ \bigcup_{q=1}^{w} МК_q \right\} = \left\{ \bigcup_{q=1}^{w} \left\{ \bigcup_{e=1}^{w_q} МК_{q,e} \right\} \right\} = \\ &= \left\{ \bigcup_{q=1}^{w} \left\{ \bigcup_{e=1}^{w_q} \left\{ \bigcup_{y=1}^{w_{q,e}} МК_{q,e,y} \right\} \right\} \right\} = \\ &= \left\{ \bigcup_{q=1}^{w} \left\{ \bigcup_{e=1}^{w_q} \{МК_{q,e,1}, МК_{q,e,2}, ..., МК_{q,e,w_{q,e}}\} \right\} \right\} = \\ &\left\{ \bigcup_{q=1}^{w} \{\{МК_{q,1,1} МК_{q,1,2} .... МК_{q,1,w_{q,1}}\}\{МК_{q,2,1} МК_{q,2,2} .... МК_{q,2,w_{q,2}}\}, \right. \\ &.., \left. \{МК_{q,w_q,1} МК_{q,w_q,2} .... МК_{q,w_q,w_{q,w_q}}\} \right\} = \\ &= \{\{\{МК_{1,1,1} МК_{1,1,2} .... МК_{1,1,w_{1,1}}\}, \{МК_{1,2,1} МК_{1,2,2} .... МК_{1,2,w_{1,2}}\}, .., \\ &\{МК_{1,w_1,1} МК_{1,w_1,2} .... МК_{1,w_1,w_{1,w_1}}\}\}, \{\{МК_{2,1,1} МК_{2,1,2} .... МК_{2,1,w_{2,1}}\}, \\ &\{МК_{2,2,1} МК_{2,2,2} .... МК_{2,2,w_{2,2}}\}, .., \{МК_{2,w_2,1} МК_{2,w_2,2} .... МК_{2,w_2,w_{2,w_2}}\}\}, \\ &..., \{\{МК_{w,1,1} МК_{w,1,2} .... МК_{w,1,w_{w,1}}\}, \{МК_{w,2,1} МК_{w,2,2} .... МК_{w,2,w_{w,2}}\}, \\ &.., \{МК_{w,w_w,1} МК_{w,w_w,2} .... МК_{w,w_w,w_{w,w_w}}\}\}. \end{aligned} \quad (5)$$

5. Formation of the method of identification of FSP

Step 1. Formation of the primary set of functional security services.

As previously described, the levels of the elements of the sets of criteria are determined by $МК_{q,e,y}$ where $y = \overline{1,w_{q,e}}$ – y-th level of $МК_{q,e}$-th element of $МК_q$ - th set criteria and $w_{q,e}$ its maximum level. Thus, we define the primary set (PS) of functional security services (FSS) as the union of elements of sets of criteria defined by the expert:

$$ПМ_p = \left\{ \bigcup_{f=1}^{k} ПМ_{p,f} \right\} = \{ПМ_{p,1}, ПМ_{p,2} ..., ПМ_{p,k}\}, \quad (6)$$

where k - the number of primary projects [2] identified by the expert.

Step 2. Formation of secondary sets of functional security services.

Next, we form an FSSSS, which consists elements of a set of criteria МК, that have levels that characterize the FSS according to [9]. In turn, the FFP function is intended to display from a set of PS into one or more elements of the set МК by means of which can form a set of all possible functions from the elements, $ПМ_f$, $f = \overline{1,k}$. We define the number of SS of the FSS:

$$\begin{aligned} ВМ_p &= \left\{ \bigcup_{f=1}^{k} ВМ_{p,f} \right\} = \left\{ \bigcup_{f=1}^{k} ФВП(ПМ_{p,f}) \right\} = \\ &= \{ВМ_{p,1}, ВМ_{p,2}, ..., ВМ_{p,k}\} = \\ &= \{ФВП(ПМ_{p,1}), ФВП(ПМ_{p,2}), ..., ФВП(ПМ_{p,k})\}, \end{aligned} \quad (7)$$

where k − respectively, the number of secondary

functional security services of the project and mapping from the set of PS to one or more elements of the $_{МК}$ set of the project.

Step 3. Formation of a basic FSP**.**

The Basic Functional Security Profile (FSP), given the expertise and facility requirements to ensure the safe flow of information, consists of a set of primary (PS) and secondary (SS) FSS. Let us define the FSP:

$$БЗ_р = \left\{\left\{\bigcup_{f=1}^{k} ФВП(ПМ_{p,f})\right\}, \left\{\bigcup_{f=1}^{k} ВМ_{p,f}\right\}\right\} =$$

$$= \left\{\left\{ФВП(ПМ_{p,1}), ФВП(ПМ_{p,2}),.., ФВП(ПМ_{p,k})\right\},\right.$$

$$\left.\left\{ВМ_{p,1}, ВМ_{p,2},.., ВМ_{p,k}\right\}\right\},$$

where $БЗ_р$ - basic functional profile of protection of the project.

Step 4. Forming a set of order by element indices $МК_{q,e,y}$

Using (6), taking into account [9], we form a set of order by indices:

$$БЗ_{ППМЕ} = \{МК_{1,1,4},\ МК_{1,2,4},\ МК_{1,3,2},\ МК_{2,1,4}, МК_{2,2,4},$$
$$МК_{2,3,2}, МК_{2,4,3},\ МК_{3,1,3}, МК_{3,2,3},\ МК_{3,3,3}, МК_{3,4,3},$$
$$МК_{4,1,5}, МК_{4,2,2}, МК_{4,3,2}\ , МК_{4,4,3}, МК_{4,5,3}, МК_{4,6,2},$$
$$МК_{4,8,1},\ МК_{4,9,1}\} = \{КД\text{-}4, КА\text{-}4, КО\text{-}1, КК\text{-}2, КВ\text{-}4,$$
$$ЦД\text{-}4, ЦА\text{-}4, ЦО\text{-}2, ЦВ\text{-}3, ДР\text{-}3, ДС\text{-}3, ДЗ\text{-}3, ДВ\text{-}3,$$
$$НР\text{-}5, НИ\text{-}2, НК\text{-}2, НО\text{-}3, НЦ\text{-}3, НТ\text{-}2, НА\text{-}1,$$
$$НП\text{-}1, НВ\text{-}2, НА\text{-}1, НП\text{-}1\}$$

Step 5. Minimizing the basic FSP

Using (7) taking into account [9] we minimize the basic FPP by the highest y-th index:

$$БЗ_р^{min} = \left\{\bigcup_{q=1}^{w}\left\{\bigcup_{e=1}^{w_q}\left\{\bigvee_{y=1}^{w_{q,e}} МК_{q,e,y}\right\}\right\}\right\} =$$

$$= \left\{\bigcup_{q=1}^{w}\left\{\bigcup_{e=1}^{w_q}\left\{МК_{q,e,1}\vee, МК_{q,e,2}\vee,..., \vee МК_{q,e,w_{q,e}}\right\}\right\}\right\} =$$

$$= \left\{\bigcup_{q=1}^{w}\left\{\left\{МК_{q,1,1}\vee, МК_{q,1,2}\vee,..., \vee МК_{q,1,w_{q,1}}\right\}\right.\right.$$
$$\left\{МК_{q,2,1}\vee, МК_{q,2,2}\vee,..., \vee МК_{q,2,w_{q,2}}\right\},..,$$
$$\left.\left.\left\{МК_{q,w_q,1}\vee, МК_{q,w_q,2}\vee,..., \vee МК_{q,w_q,w_{q,w_q}}\right\}\right\}\right\} =$$
$$= \left\{\left\{\left\{МК_{1,1,1}\vee, МК_{1,1,2}\vee,..., \vee МК_{1,1,w_{1,1}}\right\},\right.\right.$$
$$\left\{МК_{1,2,1}\vee, МК_{1,2,2}\vee,..., \vee МК_{1,2,w_{1,2}}\right\},..,$$
$$\left.\left\{МК_{1,w_1,1}\vee, МК_{1,w_1,2}\vee,..., \vee МК_{1,w_1,w_1}\right\}\right\},$$
$$\left\{\left\{МК_{2,1,1}\vee, МК_{2,1,2}\vee,..., \vee МК_{2,1,w_{2,1}}\right\},\right.$$
$$\left\{МК_{2,2,1}\vee, МК_{2,2,2}\vee,..., \vee МК_{2,2,w_{2,2}}\right\},...$$
$$\left.\left\{МК_{2,w_2,1}\vee, МК_{2,w_2,2}.\vee ..., \vee МК_{2,w_2,w_2}\right\}\right\},...,$$
$$\left\{\left\{МК_{w,1,1}\vee, МК_{w,1,2}\vee,..., \vee МК_{w,1,w_{w,1}}\right\},\right.$$
$$\left\{МК_{w,2,1}\vee, МК_{w,2,2}\vee,..., \vee МК_{w,2,w_{w,2}}\right\},..,$$
$$\left.\left.\left\{МК_{w,w_w,1}\vee, МК_{w,w_w,2}\vee,..., \vee МК_{w,w_w,w_{w,w_w}}\right\}\right\}\right\}, \qquad (8)$$

As a result, I have developed a system that analyzes the input documents for the presence of a FSP and its identification by the formal characteristics of the [9].

In case of errors, corrects FSP. The system is implemented on the .NET platform in C# programming language using the Microsoft Visual Studio development environment.

The implementation of a software module for identifying a functional security profile is intended to assist the expert in identifying the FSP in a Microsoft Word document, and to assist the expert in the analysis of the FSP. The main purpose of this software module is to assist the expert in the creation of the FSP and to control compliance with the conditions set out in the regulatory document [9], namely: determination of integrity control; takeovers by the highest FSS of lower ones; checking the correlation of the FSS.

The software module is written in C# programming language in VisualStudio 2005. In the written code technology used MSOffice'sCOMInterop, namely Microsoft.Office.Interop.Word library and basic libraries of programming language C#.

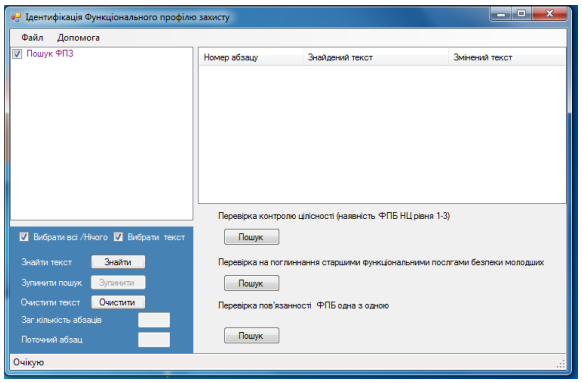

Figure 1: Program interface

The interface of the program module (Fig. 1) is a window application, which is implemented in the form of a GUI program, in which there are the following controls: a window box type "Listbox" search for a functional security profile; buttons: "Find", "Stop", "Clear"; the right part of the screen has a window of type "ListView", which displays the paragraph number where the FPP was found and the security profile found; three buttons to search for compliance of the FPP with the terms of the regulatory document [9]; two textboxes of type "TextBox" in one of which the total number of paragraphs of the document is displayed, and in the other field the current paragraph when processing the document; a «statusStrip» type window with three positions: "Pending", "Search started", "Search

is complete"; two window boxes of the type "CheckedBox" in one of which there is a possibility to deselect or select the search of the FSP, and in the other field there is an opportunity to go to the specified part of the FSP search text; window menu type "menuStrip", which contains two tabs: "File", "Help".

Microsoft Word is a specialized hierarchical, COM-oriented data warehouse - Structured Storage. A document can contain different types of data: structured text, graphics, mathematical expressions, organizational charts, etc. The concept of structured repository is an integral part of the modern programming paradigm based on the Component Object Model (COM). In fact, structured storage is the technology of combining objects (files) of objects with different nature and properties into one logical unit of storage. COM technology offers the standard implementation of the concept of structured storage in the form of a compound file (Compound File): a file system inside the file. The COM repository is a hierarchical structure of collections of objects of two types: Storage and Stream, to which directories and files correspond in the traditional file system. This approach can significantly reduce the storage costs in a single file of objects of different nature.

The implementation of the program includes methods of regular expressions: comparison of strings; suffix tree; approximating patterns; patterns with which multiple choices can be made, partial patterns. It is shown that technologies that combine the properties of approximating patterns and patterns by which multiple choice can be made, solve the problems of FSP analysis and can be used to build a system.

Testing of the program module was carried out in the process of the state examination of the CISS Grid site. The work of the software module resulted in the fulfillment of the tasks for the search of the FSP and analysis of the FSP for compliance with the three conditions. Performance analysis using the software module showed a multiple increase in the speed of document processing in the absence of errors, namely - the software module eliminated the repetition of the FSS, performed a check of integrity and completeness. The analysis of execution with the help of the program showed many increase of speed of processing of the document at 100% absence of errors, namely, the program excluded inclusion in the FPP of the same type of services, performed the check of integrity and completeness. Approximate time of processing of documents was: Technical task - 17 sec; Explanatory note to the technical project - 43 seconds; Act of inspection - 7 sec .; Information Security Policy - 12 sec. The program was run on a workstation with the following specifications: Intel Core i5-4670 CPU with 3.4 GHz; RAM - 8 GB.

The volume of the document is 8635 words. The average speed of reading in Ukrainian in an adult is within 150-200 words per minute [10], according to experimental studies, the average speed is 201 words per minute (with scatter of values from 60 to 378) with an average percentage of mastering 52 words per minute. Table 1 summarizes the time required for the expert to process the standard inputs of the CISS examination. It is only 43 minutes to read the “Terms of Reference”. Analysis time depends on the experience of the expert and can not be less than reading time. Therefore, the acceleration of processing will be at about fifteen thousand percent.

Table 1

Time required to process documents

Document Name	The total number of words	Minimum Read Time (min)
Terms of Reference	8635	43
Explanatory note to technical project	22641	113
Inspection Act	2235	11
Information Security Policy	5206	26

Let’s consider software features. Software Components:

1. Knowledge base;
2. User interface;
3. Software module "Meaning constants";
4. Software module "FSP Identification";
5. Software module “Determination of FSP";

Meaning Constants module. The module should ensure that semantic constants are extracted from the input documents by forming a set of defined constants in the knowledge base and inserting these constants into the output document templates by a defined algorithm.

The Subsystem of Meaning Constants module performs the following functions:

• selection of semantic constants from input documents;

• formation of knowledge base of semantic constants;

• Completing source document templates.

Module « FSP Determination» ensures that the FSP complies with the three criteria of RD STPI 2.5.004-99 [9]. The subsystem "Determination of FSP" ensures the following functions:

The FSP is obliged to include the control of the integrity of the STPI:

• the connection of the FSP to each other according to the RD STPI 2.5.004-99;

• if the service has any too FSS or more, then FSP can include only one functional security service.

FSP Identification Module

The module should ensure the formal compliance of the PSP with the format of the FSS description, as well as give the expert, in an interactive mode, the possibility to analyze the FSP in accordance with the normative document of the RD STPI 2.5.004-99.

The subsystem "Determination of FSP" must ensure the following functions:

• check the description of the FSP;

• provide the expert with the opportunity to receive extended information about the service in an interactive mode at events of type mouse focus.

According to testing methods, one can classify, for example, as black box testing or behavioral testing - a strategy (method) for testing the functional behavior of an object (program, system) from the point of view of the outside world, in which knowledge about the internal structure of the tested object is not used. Strategy refers to systematic methods for selecting and creating tests for a test suite. The behavioral test strategy is based on technical requirements and their specifications [2,11,12]. The "black box" refers to the object of study, the internal structure of which is unknown. The concept of a “black box” was proposed by Ashby, William Ross. In cybernetics, it allows you to study the behavior of systems, that is, their reactions to a variety of external influences and at the same time abstract from their internal structure. Manipulating only with inputs and outputs, it is possible to conduct certain studies. In practice, the question always arises of how the black box homomorphism reflects the adequacy of its studied model, that is, how fully the basic properties of the original are reflected in the model. The description of any control system in time is characterized by a picture of the sequence of its states in the process of moving toward its goal. The transformation in the control system can be either one-to-one and then it is called isomorphic, or only unambiguous, in one direction. In this case, the transformation is called homomorphic. The “black” box is a complex homomorphic model of a cybernetic system in which diversity is respected. It is only then a satisfactory system model when it contains such an amount of information that reflects the diversity of the system. It can be assumed that the greater the number of perturbations acting on the inputs of the system model, the greater the variety the regulator should have. Currently, two types of "black" boxes are known. The first type includes any “black” box, which can be considered as an automaton, called finite or infinite. The behavior of such "black" boxes is known. The second type includes such "black" boxes, whose behavior can be observed only in the experiment. In this case, a hypothesis is expressed explicitly or implicitly about the predictability of the behavior of the black box in a probabilistic sense. Without a preliminary hypothesis, any generalization is impossible, or, as they say, it is impossible to draw an inductive conclusion based on experiments with the black box. To designate the model of the “black” box, N. Wiener proposed the concept of a “white” box. The “white” box consists of known components, that is, known X, Y, δ, λ. Its contents are specially selected to implement the same dependence of the output on the input as the corresponding "black" box. In the process of research and generalizations, hypotheses and establishing patterns, it becomes necessary to adjust the organization of the “white” box and change models. In this regard, when modeling, the researcher must necessarily repeatedly refer to the scheme of relations “black” - “white” box. Creating a mathematical description of a black box is a kind of art. In some cases, it is possible to form an algorithm in accordance with which the “black” box responds to an arbitrary input signal. The main methods of testing a black box are: – equivalent partition; – analysis of boundary values; – analysis of cause and effect relationships; – assumption of error. A tester with extensive experience seeks out errors without any methods, but at the same time, he unconsciously uses the method of assuming an error. This method is largely based on intuition. The main idea of the method is to make a list that lists possible errors and situations in which these errors could occur. Then, based on the list, tests are compiled.It’s possible that it’s more correct to talk

about different degrees of transparency, and maybe even generally about different colors of the box, rather than testing using the black method and the white box method. The only important thing is what information we take into account when designing tests. Either we use information about the internal structure of the program, or we do not use it. The following CISS components were subject to testing:

1) OS protection and administration tools;

2) security features (security services) of middleware;

3) means of increasing accessibility;

4) organizational measures to protect information, software and hardware;

5) documentation on CISS according to the list defined by the requirements of TR.

The purpose of the CISS tests are:

- verification of the implementation and sufficiency of organizational measures of protection given in the documentation;

- verification of compliance with the requirements of section 10 "Criteria of guarantees" RD STPI 2.5-004-99 for the level of guarantees of the correct implementation of the G2 security functions in relation to the CIS architecture, CIS development environment, CIS development sequence, CIS functioning environment, documentation and tests of CIS.

Verification of compliance with the conditions for the implementation of information security services is carried out in accordance with the FSP:

3.КЦД = {КА-2, КД-2, КВ-1, ЦА-1 , ЦД-1, ЦВ-1, ДС-1, ДЗ-2, ДВ-1, НР-2, НИ-2, НК-1, НО-1, НЦ-2, НТ-2, НВ-1}

6. Conclusion

The paper offers a model of parameters which due to the theoretical and multiple representation of certain sets of criteria for information security, their elements and corresponding levels, allowed to formally form the necessary set of values for the implementation of the identification of FSP in the CS. In addition, a method for identifying the FSP was developed which made it possible to automate the process of determining requirements [9] for security features (security services) and guarantees. As a result, a software module was created that eliminates the repetition of the FSS, performed integrity and completeness checks.

7. References

[1] About information: Law of Ukraine of October 2, 1992 No. 2657-XII, ed. Law No. 2938 – VI of 13.01.2011. OVR, № 32, Art. 313 (2011.) (in Ukrainian).

[2] Zegzhda D.P., Ivashko A.M.: Fundamentals of security of information systems. Textbook manual for universities, p.451 (2000). (in Russian)

[3] Korchenko O.G, Davydenko A.M, Shaban M.R.: Model of parameters for identification of functional protection profile in computer systems. Security of Information. vol. 25, No.2, pp. 122-126 (2019). (in Ukrainian). DOI: https://doi.org/10.18372/2225-5036.25.13844

[4] Vysotska O., Davydenko A.: Keystroke Pattern Authentication of Computer Systems Users as One of the Steps of Multifactor Authentication. In: Hu Z., Petoukhov S., Dychka I., He M. (eds). Advances in Computer Science for Engineering and Education II. ICCSEEA 2019. Advances in Intelligent Systems and Computing, vol. 938, pp. 356-368 (2019). DOI: https://doi.org/10.1007/978-3-030-16621-2_33

[5] Kazmirchuk, S., Ilyenko A., Ilyenko S.: Digital signature authentication scheme with message recovery based on the use of elliptic curves In: Hu Z., Petoukhov S., Dychka I., He M. (eds). Advances in Computer Science for Engineering and Education II. ICCSEEA 2019. Advances in Intelligent Systems and Computing, vol. 938, pp. 279–288 (2019). DOI: https://doi.org/10.1007/978-3-030-16621-2_26

[6] Lakhno V., Kazmirchuk S., Kovalenko Y., Myrutenko L., Zhmurko T.: Design of adaptive system of detection of cyber-attacks, based on the model of logical procedures and the coverage matrices of features. Eastern-European Journal of Enterprise Technologies, vol. 3, Issue 9 (81), pp. 30–38 (2016). DOI: https://doi.org/10.15587/1729-4061.2016.71769

[7] Oleg Barabash, Oleksandr Laptiev, Valentyn Sobchuk, Ivanna Salanda, Yulia Melnychuk, Valerii Lishchyna. Comprehensive Methods of Evaluation of Distance Learning System Functioning. International Journal of Computer Network and Information Security (IJCNIS). Vol. 13, No. 3, Jun. 2021. pp.62-71, DOI: 10.5815/ijcnis.2021.03.06.

[8] Serhii Yevseiev, Oleksandr Laptiev, Sergii

Lazarenko, Anna Korchenko, Iryna Manzhul. Modeling the protection of personal data from trust and the amount of information on social networks. Number 1 (2021), «EUREKA: Physics and Engineering» pp.24–31. DOI:10.21303/2461-4262.2021.001615

[9] Korchenko, A., Breslavskyi, V., Yevseiev, S., ...Sievierinov, O., Tkachuk, S. Development of a Method for Constructing Linguistic Standards for Multi-Criteria Assessment of Honeypot Efficiency.Eastern-European Journal of Enterprise Technologiesthis link is disabled, 2021, 1(2(109)), pp. 14–23

[10] Serhii Yevseiev, Roman Korolyov, Andrii Tkachov, Oleksandr Laptiev, Ivan Opirskyy, Olha Soloviova. Modification of the algorithm (OFM) S-box, which provides increasing crypto resistance in the post-quantum period. International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE) Volume 9. No. 5, September-Oktober 2020, pp 8725-8729. DOI: 10.30534/ijatcse/2020/261952020.

[11] RD STPI 2.5-004-99 Criteria for evaluation of information security in computer systems against unauthorized access, approved by the Order of the Department of Special Telecommunication Systems and Information Protection of the Security Service of Ukraine dated April 28, 1999, No. 22. (in Ukrainian).

[12] Korchenko O.G., Davydenko A.M., Shaban M.R.: A decomposition model for the representation of semantic constants and variables for the implementation of expertise in the field of STPI. Information Security, vol. 21, No.2, pp. 88-96 (2019). (in Ukrainian). DOI: https://doi.org/ 10.18372/2410-7840.21.13766